

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

07.04.00

REC'D 26 MAY 2000

WIPO

PCT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application:

1999年 4月 9日

出 願 番 号
Application Number:

平成11年特許願第103339号

出 願 人
Applicant (s):

ソニー株式会社

EKV

09/719015

PRIORITY
DOCUMENT

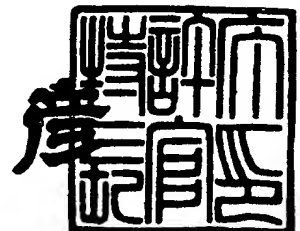
SUBMITTED OR TRANSMITTED IN
COMPLIANCE WITH RULE 17.1(a) OR (b)

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 5月12日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3034963

【書類名】 特許願

【整理番号】 9900015606

【提出日】 平成11年 4月 9日

【あて先】 特許庁長官殿

【国際特許分類】 H04L 12/16

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 石橋 義人

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 浅野 智之

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 北村 出

【発明者】

【住所又は居所】 東京都品川区北品川 6 丁目 7 番 3 5 号 ソニー株式会社
内

【氏名】 北原 淳

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代表者】 出井 伸之

【代理人】

【識別番号】 100082131

【弁理士】

【氏名又は名称】 稲本 義雄

【電話番号】 03-3369-6479

【手数料の表示】

【予納台帳番号】 032089

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9708842

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 情報処理装置および方法、並びに提供媒体

【特許請求の範囲】

【請求項 1】 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置において、

前記他の情報処理装置の所定の代理決済情報を記憶する記憶手段と、

前記記憶手段に記憶されている前記代理決済情報に対応して、所定の課金情報の提供を前記他の情報処理装置に要求する要求手段と、

前記要求手段による要求に応じて、前記他の情報処理装置から送信されてくる前記課金情報を受信する第 1 の受信手段と、

前記第 1 の受信手段により受信された前記課金情報を、前記管理装置に送信する送信手段と、

前記管理装置から送信されてくる、前記送信手段により送信された前記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第 2 の受信手段と、

前記第 2 の受信手段により受信された前記登録条件に基づいて、動作を制御する制御手段と

を備えることを特徴とする情報処理装置。

【請求項 2】 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置の情報処理方法において、

前記他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記代理決済情報に対応して、所定の課金情報の提供を前記他の情報処理装置に要求する要求ステップと、

前記要求ステップでの要求に応じて、前記他の情報処理装置から送信されてくる前記課金情報を受信する第 1 の受信ステップと、

前記第 1 の受信ステップで受信された前記課金情報を、前記管理装置に送信する送信ステップと、

前記管理装置から送信されてくる、前記送信ステップで送信された前記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受

信する第2の受信ステップと、

前記第2の受信ステップで受信された前記登録条件に基づいて、動作を制御する制御ステップと

を含むことを特徴とする情報処理方法。

【請求項3】 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置に、

前記他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、

前記記憶ステップで記憶された前記代理決済情報に対応して、所定の課金情報の提供を前記他の情報処理装置に要求する要求ステップと、

前記要求ステップでの要求に応じて、前記他の情報処理装置から送信されてくる前記課金情報を受信する第1の受信ステップと、

前記第1の受信ステップで受信された前記課金情報を、前記管理装置に送信する送信ステップと、

前記管理装置から送信されてくる、前記送信ステップで送信された前記課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信ステップと、

前記第2の受信ステップで受信された前記登録条件に基づいて、動作を制御する制御ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【請求項4】 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置において、

前記他の情報処理装置の所定の代理購入情報を記憶する第1の記憶手段と、

前記第1の記憶手段に記憶されている前記代理購入情報に対応して、所定の課金情報を作成する第1の作成手段と、

前記第1の記憶手段に記憶されている前記代理購入情報に対応して、所定の使用許諾条件情報を作成する第2の作成手段と、

前記第1の作成手段により作成された前記課金情報を記憶する第2の記憶手段と、

前記第2の作成手段により作成された前記使用許諾条件情報と、前記管理装置から供給された、暗号化された前記情報を復号するために必要な鍵を、前記他の情報処理装置に送信する送信手段と

を備えることを特徴とする情報処理装置。

【請求項5】 前記他の情報処理装置が、
 所定の表示を制御する表示手段と、
 所定のデータの入力を制御する入力制御手段と
 を備えているとき、
 前記第1の作成手段は、前記表示手段により制御された前記表示が参照されて、前記入力制御手段に入力されたデータに基づいて、前記課金情報を作成し、
 前記第2の作成手段は、前記表示手段により制御された前記表示が参照されて、前記入力制御手段に制御された前記データに基づいて、前記使用許諾条件情報を作成する

ことを特徴とする請求項4に記載の情報処理装置。

【請求項6】 他の情報処理装置に接続され、かつ、管理装置に管理されて、暗号化された情報を復号して利用する情報処理装置の情報処理方法において、前記他の情報処理装置の所定の代理購入情報を記憶する第1の記憶ステップと

前記第1の記憶ステップで記憶された前記代理購入情報に対応して、所定の課金情報を作成する第1の作成ステップと、

前記第1の記憶ステップで記憶された前記代理購入情報に対応して、所定の使用許諾条件情報を作成する第2の作成ステップと、

前記第1の作成ステップで作成された前記課金情報を記憶する第2の記憶ステップと、

前記第2の作成ステップで作成された前記使用許諾条件情報と、前記管理装置から供給された、暗号化された前記情報を復号するために必要な鍵を、前記他の情報処理装置に送信する送信ステップと

を含むことを特徴とする情報処理方法。

【請求項7】 他の情報処理装置に接続され、かつ、管理装置に管理されて

、暗号化された情報を復号して利用する情報処理装置に、

前記他の情報処理装置の所定の代理購入情報を記憶する第 1 の記憶ステップと

前記第 1 の記憶ステップで記憶された前記代理購入情報に対応して、所定の課金情報を作成する第 1 の作成ステップと、

前記第 1 の記憶ステップで記憶された前記代理購入情報に対応して、所定の使用許諾条件情報を作成する第 2 の作成ステップと、

前記第 1 の作成ステップで作成された前記課金情報を記憶する第 2 の記憶ステップと、

前記第 2 の作成ステップで作成された前記使用許諾条件情報と、前記管理装置から供給された、暗号化された前記情報を復号するために必要な鍵を、前記他の情報処理装置に送信する送信ステップと

を含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、情報処理装置および方法、並び提供媒体に関し、特に、暗号化された情報を利用する情報処理装置および方法、並びに提供媒体に関する。

【0002】

【従来の技術】

音楽などの情報（以下、コンテンツと称する）を暗号化し、所定の契約を交わしたユーザの情報処理装置に送信し、ユーザが、情報処理装置でコンテンツを復号して、利用するシステムがある。

【0003】

【発明が解決しようとする課題】

複数の情報処理装置を有している場合、ユーザは、それぞれの情報処理装置毎に、コンテンツを購入し、その利用料金を精算しなければならず、手間がかかる課題があった。

【 0 0 0 4 】

本発明はこのような状況に鑑みてなされたものであり、ユーザが複数の情報処理装置を有している場合、主とする情報処理装置を利用して、他の情報処理装置で利用されるコンテンツを購入したり、料金の精算をすることができるようにするものである。

【 0 0 0 5 】

【課題を解決するための手段】

請求項 1 に記載の情報処理装置は、他の情報処理装置の所定の代理決済情報を記憶する記憶手段と、記憶手段に記憶されている代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求手段と、要求手段による要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第 1 の受信手段と、第 1 の受信手段により受信された課金情報を、管理装置に送信する送信手段と、管理装置から送信されてくる、送信手段により送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第 2 の受信手段と、第 2 の受信手段により受信された登録条件に基づいて、動作を制御する制御手段とを備えることを特徴とする。

【 0 0 0 6 】

請求項 2 に記載の情報処理方法は、他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、記憶ステップで記憶された代理決済情報に対応して、所定の課金情報の提供を他の情報処理装置に要求する要求ステップと、要求ステップでの要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第 1 の受信ステップと、第 1 の受信ステップで受信された課金情報を、管理装置に送信する送信ステップと、管理装置から送信されてくる、送信ステップで送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第 2 の受信ステップと、第 2 の受信ステップで受信された登録条件に基づいて、動作を制御する制御ステップとを含むことを特徴とする。

【 0 0 0 7 】

請求項 3 に記載の提供媒体は、他の情報処理装置の所定の代理決済情報を記憶する記憶ステップと、記憶ステップで記憶された代理決済情報に対応して、所定

の課金情報の提供を他の情報処理装置に要求する要求ステップと、要求ステップでの要求に応じて、他の情報処理装置から送信されてくる課金情報を受信する第1の受信ステップと、第1の受信ステップで受信された課金情報を、管理装置に送信する送信ステップと、管理装置から送信されてくる、送信ステップで送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件を受信する第2の受信ステップと、第2の受信ステップで受信された登録条件に基づいて、動作を制御する制御ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0008】

請求項1に記載の情報処理装置、請求項2に記載の情報処理方法、および請求項3に記載の提供媒体においては、他の情報処理装置の所定の代理決済情報が記憶され、記憶された代理決済情報に対応して、所定の課金情報の提供が他の情報処理装置に要求され、要求に応じて、他の情報処理装置から送信されてくる課金情報が受信され、受信された課金情報が、管理装置に送信され、管理装置から送信されてくる、送信された課金情報に基づいて行われた決済処理の結果に基づいて作成された所定の登録条件が受信され、受信された登録条件に基づいて、動作が制御される。

【0009】

請求項4に記載の情報処理装置は、他の情報処理装置の所定の代理購入情報を記憶する第1の記憶手段と、第1の記憶手段に記憶されている代理購入情報に対応して、所定の課金情報を作成する第1の作成手段と、第1の記憶手段に記憶されている代理購入情報に対応して、所定の使用許諾条件情報を作成する第2の作成手段と、第1の作成手段により作成された課金情報を記憶する第2の記憶手段と、第2の作成手段により作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【0010】

請求項6に記載の情報処理方法は、他の情報処理装置の所定の代理購入情報を記憶する第1の記憶ステップと、第1の記憶ステップで記憶された代理購入情報

に対応して、所定の課金情報を作成する第 1 の作成ステップと、第 1 の記憶ステップで記憶された代理購入情報に対応して、所定の使用許諾条件情報を作成する第 2 の作成ステップと、第 1 の作成ステップで作成された課金情報を記憶する第 2 の記憶ステップと、第 2 の作成ステップで作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信ステップとを含むことを特徴とする。

【0011】

請求項 7 に記載の提供媒体は、他の情報処理装置の所定の代理購入情報を記憶する第 1 の記憶ステップと、第 1 の記憶ステップで記憶された代理購入情報に対応して、所定の課金情報を作成する第 1 の作成ステップと、第 1 の記憶ステップで記憶された代理購入情報に対応して、所定の使用許諾条件情報を作成する第 2 の作成ステップと、第 1 の作成ステップで作成された課金情報を記憶する第 2 の記憶ステップと、第 2 の作成ステップで作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信ステップとを含む処理を実行させるコンピュータが読み取り可能なプログラムを提供することを特徴とする。

【0012】

請求項 4 に記載の情報処理装置、請求項 6 に記載の情報処理方法、および請求項 7 に記載の提供媒体においては、他の情報処理装置の所定の代理購入情報が記憶され、記憶されている代理購入情報に対応して、所定の課金情報が作成され、記憶されている代理購入情報に対応して、所定の使用許諾条件情報が作成され、作成された課金情報が記憶され、作成された使用許諾条件情報と、管理装置から供給された、暗号化された情報を復号するために必要な鍵を、他の情報処理装置に送信する送信手段とを備えることを特徴とする。

【0013】

【発明の実施の形態】

以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次

のようになる。但し勿論この記載は、各手段を記載したものに限定することを意味するものではない。

【0014】

図1は、本発明を適用したEMD(Electronic Music Distribution:電子音楽配信)システムを説明する図である。EMDシステムは、各装置を管理するEMDサービスセンタ1、コンテンツを提供するコンテンツプロバイダ2、コンテンツに対応する所定のサービスを提供するサービスプロバイダ3、およびコンテンツが利用される機器(この例の場合、HDD52に接続されているレシーバ51およびHDD202に接続されているレシーバ201)からなるユーザネットワーク5から構成されている。

【0015】

EMDシステムにおけるコンテンツ(Content)とは、情報そのものが価値を有するデジタルデータで、この例の場合、1つのコンテンツは、1曲分の音楽データに相当する。

【0016】

EMDサービスセンタ1は、EMDシステムにおける主な情報の流れを示す図2に示すように、ユーザホームネットワーク5およびコンテンツプロバイダ2に、コンテンツを利用するために必要な配送用鍵Kdを送信する。EMDサービスセンタ1はまた、ユーザホームネットワーク5の機器から、課金情報等を受信して、料金を精算する処理などを実行する。

【0017】

コンテンツプロバイダ2は、提供するコンテンツ(コンテンツ鍵Kcoで暗号化されている)、そのコンテンツを復号するために必要なコンテンツ鍵Kco(配送用鍵Kdで暗号化されている)、およびコンテンツの利用内容などを示す取扱方針(以下、UCP(Usage Control Policy)と記述する)を保持し、それらを、コンテンツプロバイダセキュアコンテナ(後述)と称する形態で、サービスプロバイダ3に供給する。

【0018】

サービスプロバイダ3は、コンテンツプロバイダ2から供給されるUCPの利用

内容に対応して、1つまたは複数の価格情報（以下、PT(Price Tag)と記述する）を作成し、保持する。サービスプロバイダ2は、作成したPTを、コンテンツプロバイダ2から供給されたコンテンツ（コンテンツ鍵K_cで暗号化されている）、コンテンツ鍵K_c（配送用鍵K_dで暗号化されている）、およびUCPとともに、サービスプロバイダセキュアコンテナと称する形態で、専用のケーブルネットワーク、インターネット、または衛星通信などから構成されるネットワーク4を介して、ユーザホームネットワーク5に送信する。

【0019】

ユーザホームネットワーク5は、供給されたUCPおよびPTに基づいて、使用許諾条件情報（以下、UCS(Usage Control Status)と称する）を作成し、作成したUCSに基づいてコンテンツを利用する処理を実行する。ユーザホームネットワーク5はまた、UCSを作成するタイミングで課金情報を作成し、例えば、配送用鍵K_dの供給を受けるタイミングで、EMDサービスセンタ1に送信する。

【0020】

図3は、EMDサービスセンタ1の機能的構成を示すブロック図である。サービスプロバイダ管理部11は、サービスプロバイダ3に利益分配の情報を供給する。コンテンツプロバイダ管理部12は、コンテンツプロバイダ2に配送用鍵K_dを送信したり、利益分配の情報を供給する。

【0021】

著作権管理部13は、ユーザホームネットワーク5のコンテンツの利用の実績を示す情報を、著作権を管理する団体、例えば、JASRAC(Japanese Society for Rights of Authors, Composers and Publishers:日本音楽著作権協会)に送信する。

【0022】

鍵サーバ14は、配送用鍵K_dを記憶しており、それを、コンテンツプロバイダ管理部12を介してコンテンツプロバイダ2に供給したり、ユーザ管理部18等を介してユーザホームネットワーク5に供給する。

【0023】

ユーザホームネットワーク 5 の機器およびコンテンツプロバイダ 2 に供給される、EMD サービスセンタ 1 からの配送用鍵 K d について、図 4 乃至図 7 を参照して説明する。

【0024】

図 4 は、コンテンツプロバイダ 2 がコンテンツの提供を開始し、ユーザホームネットワーク 5 を構成するレシーバ 5 1 がコンテンツの利用を開始する、1998 年 1 月における、EMD サービスセンタ 1 が有する配送用鍵 K d、コンテンツプロバイダ 2 が有する配送用鍵 K d、およびレシーバ 5 1 が有する配送用鍵 K d を示す図である。

【0025】

図 4 の例において、配送用鍵 K d は、暦の月の初日から月の末日まで、使用可能であり、たとえば、所定のビット数の乱数である” a a a a a a a a ” の値を有するバージョン 1 である配送用鍵 K d は、1998 年 1 月 1 日から 1998 年 1 月 31 日まで使用可能（すなわち、1998 年 1 月 1 日から 1998 年 1 月 31 日の期間にサービスプロバイダ 3 を介してユーザホームネットワーク 5 に配布されるコンテンツを暗号化するコンテンツ鍵 K c o は、バージョン 1 である配送用鍵 K d で暗号化されている）であり、所定のビット数の乱数である” b b b b b b b b ” の値を有するバージョン 2 である配送用鍵 K d は、1998 年 2 月 1 日から 1998 年 2 月 28 日まで使用可能（すなわち、その期間にサービスプロバイダ 3 を介してユーザホームネットワーク 5 に配布されるコンテンツを暗号化するコンテンツ鍵 K c o は、バージョン 2 である配送用鍵 K d で暗号化されている）である。同様に、バージョン 3 である配送用鍵 K d は、1998 年 3 月中に使用可能であり、バージョン 4 である配送用鍵 K d は、1998 年 4 月中に使用可能であり、バージョン 5 である配送用鍵 K d は、1998 年 5 月中に使用可能であり、バージョン 6 である配送用鍵 K d は、1998 年 6 月中に使用可能である。

【0026】

コンテンツプロバイダ 2 がコンテンツの提供を開始するに先立ち、EMD サービスセンタ 1 は、コンテンツプロバイダ 2 に、1998 年 1 月から 1998 年 6 月

まで利用可能な、バージョン1乃至バージョン6の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、記憶する。6月分の配送用鍵Kdを記憶するのは、コンテンツプロバイダ2が、コンテンツを提供する前のコンテンツおよびコンテンツ鍵の暗号化などの準備に、所定の期間が必要だからである。

【0027】

また、レシーバ51がコンテンツの利用を開始するに先立ち、EMDサービスセンタ1は、レシーバ51に、1998年1月から1998年3月まで、利用可能なバージョン1乃至バージョン3である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、記憶する。3月分の配送用鍵Kdを記憶するのは、レシーバ51が、EMDサービスセンタ1に接続できないなどのトラブルにより、コンテンツの利用が可能な契約期間にもかかわらずコンテンツが利用できない等の事態を避けるためであり、また、EMDサービスセンタ1への接続の頻度を低くし、ユーザホームネットワーク5の負荷を低減するためである。

【0028】

1998年1月1日から1998年1月31日の期間には、バージョン1である配送用鍵Kdが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0029】

1998年2月1日における、EMDサービスセンタ1の配送用鍵Kdのコンテンツプロバイダ2、およびレシーバ51への送信を図5で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年2月から1998年7月まで利用可能な、バージョン2乃至バージョン7の6つの配送用鍵Kdを送信し、コンテンツプロバイダ2は、6つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年2月から1998年4月まで、利用可能なバージョン2乃至バージョン4である3つの配送用鍵Kdを送信し、レシーバ51は、3つの配送用鍵Kdを受信し、受信前に記憶していた配送用鍵Kdに上書きし、新たな配送用鍵Kdを記憶する。EMDサービスセンタ1は、バージョン

1である配送用鍵K dをそのまま記憶する。これは、不測のトラブルが発生したとき、若しくは不正が発生し、または発見されたときに、過去に利用した配送用鍵K dを利用できるようにするためである。

【0030】

1998年2月1日から1998年2月28日の期間には、バージョン2である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0031】

1998年3月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図6で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年3月から1998年8月まで利用可能な、バージョン3乃至バージョン8の6つの配送用鍵K dを送信し、コンテンツプロバイダ2は、6つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、レシーバ51に、1998年3月から1998年5月まで、利用可能なバージョン3乃至バージョン5である3つの配送用鍵K dを送信し、レシーバ51は、3つの配送用鍵K dを受信し、受信前に記憶していた配送用鍵K dに上書きし、新たな配送用鍵K dを記憶する。EMDサービスセンタ1は、バージョン1である配送用鍵K dおよびバージョン2である配送用鍵K dをそのまま記憶する。

【0032】

1998年3月1日から1998年3月31日の期間には、バージョン3である配送用鍵K dが、EMDサービスセンタ1、コンテンツプロバイダ2、ユーザホームネットワーク5を構成するレシーバ51で利用される。

【0033】

1998年4月1日における、EMDサービスセンタ1の配送用鍵K dのコンテンツプロバイダ2、およびレシーバ51への送信を図7で説明する。EMDサービスセンタ1は、コンテンツプロバイダ2に、1998年4月から1998年9月まで利用可能な、バージョン4乃至バージョン9の6つの配送用鍵K dを送信し

、コンテンツプロバイダ 2 は、6 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、レシーバ 5 1 に、1 9 9 8 年 4 月から 1 9 9 8 年 6 月まで、利用可能なバージョン 3 乃至バージョン 5 である 3 つの配送用鍵 K d を送信し、レシーバ 5 1 は、3 つの配送用鍵 K d を受信し、受信前に記憶していた配送用鍵 K d に上書きし、新たな配送用鍵 K d を記憶する。EMD サービスセンタ 1 は、バージョン 1 である配送用鍵 K d、バージョン 2 である配送用鍵 K d、およびバージョン 3 である配送用鍵 K d をそのまま記憶する。

【 0 0 3 4 】

1 9 9 8 年 4 月 1 日から 1 9 9 8 年 4 月 3 0 日の期間には、バージョン 4 である配送用鍵 K d が、EMD サービスセンタ 1、コンテンツプロバイダ 2、ユーザホームネットワーク 5 を構成するレシーバ 5 1 で利用される。

【 0 0 3 5 】

このように、あらかじめ先の月の配送用鍵 K d を配布しておくことで、仮にユーザが 1、2 ヶ月まったく EMD サービスセンタ 1 にアクセスしていなくても、一応、コンテンツの買い取りが行え、時を見計らって、EMD サービスセンタ 1 にアクセスして鍵を受信することができる。

【 0 0 3 6 】

図 3 に戻り、経歴データ管理部 1 5 は、ユーザ管理部 1 8 から出力される、課金情報、そのコンテンツに対応する PT、およびそのコンテンツに対応する UCP などを記憶する。

【 0 0 3 7 】

利益分配部 1 6 は、経歴データ管理部 1 5 から供給された各種情報に基づき、EMD サービスセンタ 1、コンテンツプロバイダ 2、およびサービスプロバイダ 3 の利益をそれぞれ算出し、その結果をサービスプロバイダ管理部 1 1、コンテンツプロバイダ管理部 1 2、出納部 2 0、および著作権管理部 1 3 に出力する。

【 0 0 3 8 】

相互認証部 1 7 は、コンテンツプロバイダ 2、サービスプロバイダ 3、およびユーザホームネットワーク 5 の機器と相互認証を実行する。ユーザ管理部 1 8 は

、所定の処理に対応して登録リスト（後述）を作成し、配送用鍵K_dとともにユーザホームネットワーク5に送信する。

【0039】

課金請求部19は、経歴データ管理部15から供給された、例えば、課金情報、UCP、およびPTに基づき、ユーザへの課金を算出し、その結果を、出納部20に供給する。出納部20は、ユーザ、コンテンツプロバイダ2、およびサービスプロバイダ3への出金、徴収すべき利用料金の金額を基に、図示せぬ外部の銀行等と通信し、決算処理を実行する。出納部20はまた、決算処理の結果をユーザ管理部18に通知する。

【0040】

監査部21は、ユーザホームネットワーク5の機器から供給された課金情報、PT、およびUCPの正当性（すなわち、不正をしていないか）を監査する。なお、この場合、EMDサービスセンタ1は、コンテンツプロバイダ2からのUCPを、サービスプロバイダ3からのPTを、そしてユーザホームネットワーク5からのUCPとPTを、それぞれ受け取る。

【0041】

図8は、コンテンツプロバイダ2の機能的構成を示すブロック図である。コンテンツサーバ31は、ユーザに供給するコンテンツを記憶し、ウォーターマーク付加部32に供給する。ウォーターマーク付加部32は、コンテンツサーバ31から供給されたコンテンツにウォーターマーク（電子透かし）を付加し、圧縮部33に供給する。

【0042】

圧縮部33は、ウォーターマーク付加部32から供給されたコンテンツを、ATRA C2(Adaptive Transform Acoustic Coding 2)（商標）等の方式で圧縮し、暗号化部34に供給する。暗号化部34は、圧縮部33で圧縮されたコンテンツを、乱数発生部35から供給された乱数を鍵（以下、この乱数をコンテンツ鍵K_{co}と称する）として、DES(Data Encryption Standard)などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部38に出力する。

【0043】

乱数発生部 35 は、コンテンツ鍵 K_c となる所定のビット数の乱数を暗号化部 34 および暗号化部 36 に供給する。暗号化部 36 は、コンテンツ鍵 K_c を EMD サービスセンタ 1 から供給された配送用鍵 K_d を使用して、DES などの共通鍵暗号方式で暗号化し、その結果をセキュアコンテナ作成部 38 に出力する。

【0044】

DES は、56 ビットの共通鍵を用い、平文の 64 ビットを 1 ブロックとして処理する暗号方式である。DES の処理は、平文を攪拌し、暗号文に変換する部分（データ攪拌部）と、データ攪拌部で使用する鍵（拡大鍵）を共通鍵から生成する部分（鍵処理部）からなる。DES のすべてのアルゴリズムは公開されているので、ここでは、データ攪拌部の基本的な処理を簡単に説明する。

【0045】

まず、平文の 64 ビットは、上位 32 ビットの H_0 、および下位 32 ビットの L_0 に分割される。鍵処理部から供給された 48 ビットの拡大鍵 K_1 、および下位 32 ビットの L_0 を入力とし、下位 32 ビットの L_0 を攪拌した F 関数の出力が算出される。F 関数は、数値を所定の規則で置き換える「換字」およびビット位置を所定の規則で入れ替える「転置」の 2 種類の基本変換から構成されている。次に、上位 32 ビットの H_0 と、F 関数の出力が排他的論理和され、その結果は L_1 とされる。 L_0 は、 H_1 とされる。

【0046】

上位 32 ビットの H_0 および下位 32 ビットの L_0 を基に、以上の処理を 16 回繰り返し、得られた上位 32 ビットの H_{16} および下位 32 ビットの L_{16} が暗号文として出力される。復号は、暗号化に使用した共通鍵を用いて、上記の手順を逆にたどることで実現される。

【0047】

ポリシー記憶部 37 は、コンテンツに対応して設定される UCP を記憶し、セキュアコンテナ作成部 38 に出力する。図 9 は、コンテンツサーバ 31 に保持されているコンテンツ A に対応して設定され、ポリシー記憶部 37 に記憶されている UCP A、B を表している。UCP は、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「利用条件」、「利用内容」の各項

目に対応する所定の情報が含まれる。「コンテンツのID」には、UCPに対応するコンテンツのIDが設定される。UCPA（図9（A））およびUCPB（図9（B））のそれぞれの「コンテンツのID」には、コンテンツAのIDが設定されている。

【0048】

「コンテンツプロバイダのID」には、コンテンツの提供元のコンテンツプロバイダのIDが設定される。UCPAおよびUCPBのそれぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが設定されている。「UCPのID」には、各UCPに割り当てられた所定のIDが設定され、UCPAの「UCPのID」には、UCPAのIDが、UCPBの「UCPのID」には、UCPBのIDが、それぞれ設定されている。「UCPの有効期限」には、UCPの有効期限を示す情報が設定され、UCPAの「UCPの有効期限」には、UCPAの有効期限が、UCPBの「UCPの有効期限」には、UCPBの有効期限が、それぞれ設定されている。

【0049】

「利用条件」には、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定され、「ユーザ条件」には、このUCPを選択することができるユーザの条件が設定され、「機器条件」には、このUCPを選択することができる機器の条件が設定されている。

【0050】

UCPAの場合、「利用条件10」が設定され、「利用条件10」の「ユーザ条件10」には、所定の利用ポイントが200ポイント以上が条件であることを示す情報（“200ポイント以上”）が設定されている。また「利用条件10」の「機器条件10」には、条件がないことを示す情報（“条件なし”）が設定されている。すなわち、UCPAは、200ポイント以上の利用ポイントを有するユーザのみが選択可能となる。

【0051】

UCPBの場合、「利用条件20」が設定され、「利用条件20」の「ユーザ条件20」には、所定の利用ポイントが200ポイントより少ないことが条件であることを示す情報（“200ポイントより少ない”）が設定されている。また「利用条件20」の「機器条件20」には、“条件なし”が設定されている。すな

わち、UCPBは、200ポイントより少ない利用ポイントを有するユーザのみが選択可能となる。

【0052】

「利用内容」には、「ID」、「形式」、「パラメータ」、および「管理移動許可情報」の各項目に対応する所定の情報が含まれる。「ID」には、「利用内容」に設定される情報に割り当てられた所定のIDが設定される。「形式」には、再生や複製など、コンテンツの利用形式を示す情報が設定される。「パラメータ」には、「形式」に設定された利用形式に対応する所定の情報が設定される。

【0053】

「管理移動許可情報」には、コンテンツの管理移動が可能か否か（許可されているか否かを示す情報（“可”または“不可”））が設定される。コンテンツの管理移動が行われると、図10（A）に示すように、管理移動元の機器にコンテンツが保持されつつ、管理移動先の機器にそのコンテンツが移動される。すなわち、管理移動元の機器と管理移動先の機器の両方において、コンテンツが利用される。この点で、図10（B）に示すように、移動元の機器にコンテンツが保持されず、移動先の機器のみにコンテンツが保持され、移動先の機器においてのみコンテンツが利用される、通常の移動とは異なる。

【0054】

また、コンテンツの管理移動が行われている間、管理移動元の機器は、図10（A）に示すように、他の機器にコンテンツを管理移動することができない（許可されない）。すなわち、管理移動元の機器と管理移動先の機器の2機においてのみコンテンツが保持される。この点で、図11（A）に示すように、オリジナルのコンテンツから、複数の複製（第1世代）を作成することができる、第1世代の複製とも異なる。また、管理移動元の機器からコンテンツを戻すことより、他の機器にコンテンツを管理移動することができるので、この点で、図11（B）に示すように、1回だけの複製とも異なる。

【0055】

図9（A）に戻り、UCPAには、4つの「利用内容11」乃至「利用内容14」が設けられており、「利用内容11」において、その「ID11」には、「利用

内容11」に割り当てられた所定のIDが設定されている。「形式11」には、コンテンツを買い取って再生する利用形式を示す情報（”買い取り再生”）が設定され、「パラメータ11」には、”買い取り再生”に対応する所定の情報が設定されている。「管理移動許可情報11」には、コンテンツの管理移動が許可されていることを示す情報（”可”）が設定されている。

【0056】

「利用内容12」において、その「ID12」には、「利用内容12」に割り当てられた所定のIDが設定されている。「形式12」には、第1世代の複製を行う利用形式を示す情報（”第1世代複製”）が設定されている。第1世代複製は、図11（A）に示したように、オリジナルのコンテンツから、複数の第1世代の複製を作成することができる。ただし、第1世代の複製から第2世代の複製を作成することはできない（許可されない）。「パラメータ12」には、”第1世代複製”に対応する所定の情報が設定されている。「管理移動許可情報12」には、コンテンツの管理移動が許可されていないことを示す情報（”不可”）が設定されている。

【0057】

「利用内容13」において、その「ID13」には、「利用内容13」に割り当てられた所定のIDが設定されている。「形式13」には、所定の期間（時間）に限って再生する利用形式を示す情報（”期間制限再生”）が設定され、「パラメータ13」には、”期間制限再生”に対応して、その期間の開始時期（時刻）と終了時期（時刻）が設定されている。「管理移動許可情報13」には、”不可”が設定されている。

【0058】

「利用内容14」において、その「ID14」には、「利用内容14」に割り当てられた所定のIDが設定されている。「形式14」には、5回の複製を行う利用形式を示す情報（”Pay Per Copy5”）が設定されている。なお、この場合も、図11の（B）に示すように、複製からの複製を作成することはできない（許可されない）。「パラメータ14」には、複製が5回可能であることを示す情報（”複製5回”）が設定されている。「管理移動許可情報14」には、”不可”が

設定されている。

【0059】

図9（B）のUCPBには、2つの「利用内容21」、および「利用内容22」が設けられている。「利用内容21」において、その「ID21」には、「利用内容21」に割り当てられた所定のIDが設定されている。「形式21」には、4回の再生を行う利用形式を示す情報（" Pay Per Play4 "）が設定され、「パラメータ21」には、再生が4回可能であることを示す情報" 再生4回" が設定されている。「管理移動許可情報21」には、" 不可" が設定されている。

【0060】

「利用内容22」において、その「ID22」には、「利用内容22」に割り当てられた所定のIDが設定されている。「形式22」には、" Pay Per Copy2 " が設定され、「パラメータ22」には、" 複製2回" が設定されている。「管理移動許可情報22」には、" 不可" が設定されている。

【0061】

ここで、UCPAおよびUCPBの内容を比較すると、200ポイント以上の利用ポイントを有するユーザは、4通りの利用内容11乃至利用内容14から利用内容を選択することができるのに対して、200ポイントより少ない利用ポイントを有するユーザは、2通りの利用内容21、22からしか利用内容を選択することができないものとされている。

【0062】

ところで、図9は、UCPAおよびUCPBを模擬的に表しているが、例えば、UCPAの「利用条件10」およびUCPBの「利用条件20」には、実際は、図12（A）に示すサービスコード、および図12（B）に示すコンディションコードの他、サービスコードに対応して数値や所定の種類を示すバリューコードがそれぞれ設定されている。

【0063】

図13（A）は、UCPA（図9（A））の「利用条件10」の「ユーザ条件10」および「機器条件10」として設定されている各コードのコード値を表している。UCPAの「利用条件10」の「ユーザ条件10」は、" 200ポイント以

上”とされているので、“利用ポイントに関し条件有り”を意味する 80xxh のサービスコード（図 12（A））が、このとき数値 200 を示す 0000C8h のバリューコードが、そして“>=（以上）”を意味する 06h のコンディションコード（図 12（B））が、ユーザ条件として設定されている。

【0064】

UCPA の「機器条件 10」は、“条件なし”とされているので、“条件なし”を意味する 0000h のサービスコードが、このとき何ら意味を持たない FFFFh のバリューコードが、そして“無条件”を意味する 00h のコンディションコードが、機器条件として設定されている。

【0065】

図 13（B）は、UCPB の「利用条件 20」の「ユーザ条件 20」および「機器条件 20」として設定されている各コードのコード値を表している。「ユーザ条件 20」は、“200 ポイントより少ない”とされているので、“利用ポイントに関し条件有り”を意味する 80xxh のサービスコードが、数値 200 を示す 0000C8h のバリューコードが、そして“<（より小さい）”を意味する 03h のコンディションコードが、ユーザ条件として設定されている。

【0066】

UCPB の「機器条件 20」は、UCPA の「機器条件 10」と同様に、“条件なし”とされ、同一のコード値が設定されているので、その説明は省略する。

【0067】

図 8 に戻り、セキュアコンテナ作成部 38 は、例えば、図 14 に示すような、コンテンツ A（コンテンツ鍵 Kc o A で暗号化されている）、コンテンツ鍵 Kc o A（配送用鍵 Kd で暗号化されている）、UCPA、B、および署名からなるコンテンツプロバイダセキュアコンテナを作成する。なお、署名は、送信したいデータ（この場合、コンテンツ A（コンテンツ鍵 Kc o A で暗号化されている））、コンテンツ鍵 Kc o A（配送用鍵 Kd で暗号化されている）、および UCPA、B の全体にハッシュ関数を適用して得られたハッシュ値が、公開鍵暗号の秘密鍵（この場合、コンテンツプロバイダ 2 の秘密鍵 Ks c p）で暗号化されたものである。

【0068】

セキュアコンテナ作成部 38 はまた、コンテンツプロバイダセキュアコンテナに、図 15 に示すコンテンツプロバイダ 2 の証明書を付してサービスプロバイダ 3 に送信する。この証明書は、証明書のバージョン番号、認証局がコンテンツプロバイダ 2 に対し割り付けた証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、およびコンテンツプロバイダ 2 の名前、コンテンツプロバイダ 2 の公開鍵 $K_{p,c,p}$ 、並びにその署名（認証局の秘密鍵 $K_{s,c,a}$ で暗号化されている）から構成されている。

【0069】

署名は、改竄のチェックおよび作成者認証をするためのデータであり、送信したいデータを基にハッシュ関数でハッシュ値を取り、これを公開鍵暗号の秘密鍵で暗号化して作成される。

【0070】

ハッシュ関数および署名の照合について説明する。ハッシュ関数は、送信したい所定のデータを入力とし、所定のビット長のデータに圧縮し、ハッシュ値として出力する関数である。ハッシュ関数は、ハッシュ値（出力）から入力を予測することが難しく、ハッシュ関数に入力されたデータの 1 ビットが変化したとき、ハッシュ値の多くのビットが変化し、また、同一のハッシュ値を持つ入力データを探し出すことが困難である特徴を有する。

【0071】

署名とデータを受信した受信者は、署名を公開鍵暗号の公開鍵で復号し、その結果（ハッシュ値）を得る。さらに受信されたデータのハッシュ値が計算され、計算されたハッシュ値と、署名を復号して得られたハッシュ値とが、等しいか否かが判定される。送信されたデータのハッシュ値と復号したハッシュ値が等しいと判定された場合、受信したデータは改竄されておらず、公開鍵に対応した秘密鍵を保持する送信者から送信されたデータであることがわかる。署名のハッシュ関数としては、MD4, MD5, SHA-1 などが用いられる。

【0072】

次に公開鍵暗号について説明する。暗号化および復号で同一の鍵（共通鍵）を

使用する共通鍵暗号方式に対し、公開鍵暗号方式は、暗号化に使用する鍵と復号するときの鍵が異なる。公開鍵暗号を用いる場合、鍵の一方を公開しても他方を秘密に保つことができ、公開しても良い鍵は、公開鍵と称され、他方の秘密に保つ鍵は、秘密鍵と称される。

【0073】

公開鍵暗号の中で代表的なRSA (Rivest-Shamir-Adleman) 暗号を、簡単に説明する。まず、2つの十分に大きな素数である p および q を求め、さらに p と q の積である n を求める。 $(p-1)$ と $(q-1)$ の最小公倍数 L を算出し、更に、3以上 L 未満で、かつ、 L と互いに素な数 e を求める（すなわち、 e と L を共通に割り切れる数は、1のみである）。

【0074】

次に、 L を法とする乗算に関する e の乗法逆元 d を求める。すなわち、 d 、 e 、および L の間には、 $ed=1 \bmod L$ が成立し、 d はユークリッドの互除法で算出できる。このとき、 n と e が公開鍵とされ、 p 、 q 、および d が、秘密鍵とされる。

【0075】

暗号文 C は、平文 M から、式(1)の処理で算出される。

【0076】

$$C=M^e \bmod n \quad (1)$$

暗号文 C は、式(2)の処理で平文 M に、復号される。

【0077】

$$M=C^d \bmod n \quad (2)$$

証明は省略するが、RSA暗号で平文を暗号文に変換して、それが復号できるのは、フェルマーの小定理に根拠をおいており、式(3)が成立するからである。

【0078】

$$M=C^d=(M^e)^d=M^{(ed)}=M \bmod n \quad (3)$$

秘密鍵 p と q を知っているならば、公開鍵 e から秘密鍵 d は算出できるが、公開鍵 n の素因数分解が計算量的に困難な程度に公開鍵 n の桁数を大きくすれば、公開鍵 n を知るだけでは、公開鍵 e から秘密鍵 d は計算できず、復号できない。以上のよう、RSA暗号では、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とす

ることができる。

【0079】

また、公開鍵暗号の他の例である楕円曲線暗号についても、簡単に説明する。楕円曲線 $y^2=x^3+ax+b$ 上の、ある点をBとする。楕円曲線上の点の加算を定義し、 nB は、Bをn回加算した結果を表す。同様に、減算も定義する。Bと nB からnを算出することは、困難であることが証明されている。Bと nB を公開鍵とし、nを秘密鍵とする。乱数rを用いて、暗号文C1およびC2は、平文Mから、公開鍵で式(4)および式(5)の処理で算出される。

【0080】

$$C1=M+rnB \quad (4)$$

$$C2=rB \quad (5)$$

暗号文C1およびC2は、式(6)の処理で平文Mに、復号される。

【0081】

$$M=C1-nC2 \quad (6)$$

復号できるのは、秘密鍵nを有するものだけである。以上のように、RSA暗号と同様に、楕円曲線暗号でも、暗号化に使用する鍵と復号するときの鍵を、異なる鍵とすることができる。

【0082】

図8に、再び戻り、コンテンツプロバイダ2の相互認証部39は、EMDサービスセンタ1から配送用鍵Kdの供給を受けるのに先立ち、EMDサービスセンタ1と相互認証する。また相互認証部39は、サービスプロバイダ3へのコンテンツプロバイダセキュアコンテナの送信に先立ち、サービスプロバイダ3と相互認証することも可能であるが、この例の場合、コンテンツプロバイダセキュアコンテナには、秘密しなければならない情報が含まれていないので、この相互認証は必ずしも必要とされるわけではない。

【0083】

次に、図16のブロック図を参照して、サービスプロバイダ3の機能的構成を説明する。コンテンツサーバ41は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる、コンテンツ(コンテンツ鍵K

c oで暗号化されている)、コンテンツ鍵K c o(配送用鍵K dで暗号化されている)、UCP、およびコンテンツプロバイダ2の署名を記憶し、セキュアコンテナ作成部44に供給する。

【0084】

値付け部42は、コンテンツプロバイダ2から供給されたコンテンツプロバイダセキュアコンテナに含まれる署名に基づいて、コンテンツプロバイダセキュアコンテナの正当性を検証するが、この場合、コンテンツプロバイダ2の証明書が検証され、正当であるとき、コンテンツプロバイダ2の公開鍵が取得される。そしてこの取得された公開鍵に基づいて、コンテンツプロバイダセキュアコンテナの正当性が検証される。

【0085】

コンテンツプロバイダセキュアコンテナの正当性を確認すると、値付け部42は、コンテンツプロバイダセキュアコンテナに含まれるUCPに対応する、PTを作成し、セキュアコンテナ作成部44に供給する。図17は、図9(A)のUCPAに対応して作成された、2つのPTA-1(図17(A))およびPTA-2(図17(B))を表している。PTには、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「価格条件」、および「価格内容」の各項目に対応する所定の情報が含まれる。

【0086】

PTの、「コンテンツのID」、「コンテンツプロバイダのID」、および「UCPのID」の各項目には、UCPの、これらに対応する項目の情報が、それぞれ設定される。すなわち、PTA-1およびPTA-2のそれぞれの「コンテンツのID」には、コンテンツAのIDが、それぞれの「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、そしてそれぞれの「UCPのID」には、UCPAのIDが設定されている。

【0087】

「サービスプロバイダのID」には、PTの提供元のサービスプロバイダ2のIDが設定される。PTA-1およびPTA-2のそれぞれの「サービスプロバイダのID」

には、サービスプロバイダ3のIDが設定されている。「PTのID」には、各PTに割り当てられた所定のIDが設定される。PTA-1の「PTのID」には、PTA-1のIDが、PTA-2の「PTのID」には、PTA-2のIDがそれぞれ設定されている。「PTの有効期限」には、PTの有効期限を示す情報が設定される。PTA-1の「PTの有効期限」には、PTA-1の有効期限が、PTA-2の「PTの有効期限」には、PTA-2の有効期限が設定されている。

【0088】

「価格条件」には、UCPの「利用条件」と同様に、「ユーザ条件」および「機器条件」の各項目に対応する所定の情報が設定されている。「価格条件」の「ユーザ条件」には、このPTを選択することができるユーザの条件を示す情報が設定され、その「機器条件」には、このPTを選択することができる機器の条件を示す情報が設定される。

【0089】

PTA-1の場合、「価格条件10」が設定され、「価格条件10」の「ユーザ条件10」には、ユーザが男性であることを示す情報（”男性”）が設定され、その「機器条件10」には、”条件なし”が設定されている。すなわち、PTA-1は、男性のユーザのみが選択可能となる。

【0090】

PTA-1の「価格条件10」の「ユーザ条件10」および「機器条件10」も、実際は、図18（A）に示すように、各種コードのコード値が設定されている。「価格条件10」の「ユーザ条件10」には、”性別条件有り”を意味する01xxhのサービスコード（図12（A））が、このとき男性を意味する000000hのバリューコードが、そして”=”を意味する01hのコンディションコード（図12（B））が設定されている。「機器条件10」には、”条件なし”を意味する0000hのサービスコードが、この場合何ら意味を持たないFFFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコードが設定されている。

【0091】

PTA-2の場合、「価格条件20」が設定され、「価格条件20」の「ユーザ

条件 20」には、ユーザが女性であることを示す情報（”女性”）が設定され、その「機器条件 20」には、”条件なし”が設定されている。すなわち、PTA-2 は、女性のユーザのみが選択可能となる。

【0092】

PTA-2 の「価格条件 20」の「ユーザ条件 20」および「機器条件 20」も、実際は、図 18（B）に示すように、各コードのコード値が設定されている。

「価格条件 20」の「ユーザ条件 20」には、”性別条件有り”を意味する 01xxh のサービスコード（図 12（A））が、この場合女性を示す 000001h のバリューコードが、そして”=”を意味する 01h のコンディションコード（図 12（B））が設定されている。その「機器条件 20」には、”条件なし”を意味する 0000h のサービスコードが、この場合何ら意味を持たない FFF FFFh のバリューコードが、そして”無条件”を意味する 00h のコンディションコードが設定されている。

【0093】

図 17 に戻り、PT の「価格内容」には、対応する UCP の「利用内容」の「形式」に設定されている利用形式の利用料金が示されている。すなわち、PTA-1 の「価格内容 11」に設定された”2000 円”および PTA-2 の「価格内容 21」に設定された”1000 円”は、UCPA（図 9（A））の「利用内容 11」の「形式 11」が”買い取り再生”とされているので、コンテンツ A の買い取り価格（料金）を示している。

【0094】

PTA-1 の「価格内容 12」の”600 円”および PTA-2 の「価格内容 22」の”300 円”は、UCPA の「利用内容 12」の「形式 12」より、第 1 世代複製の利用形式でコンテンツ A を利用する場合の料金を示している。PTA-1 の「価格内容 13」の”100 円”および PTA-2 の「価格内容 23」の”50 円”は、UCPA の「利用内容 13」の「形式 13」より、期間制限再生の利用形式でコンテンツ A を利用する場合の料金を示している。PTA-1 の「価格内容 14」の”300 円”および PTA-2 の「価格内容 24」の”150 円”は、UCPA の「利用内容 14」の「形式 14」より、5 回の複製を行う利用形式でコンテ

ツAを利用する場合の料金を示している。

【0095】

なお、この例の場合、PTA-1（男性ユーザに適用される）の価格内容と、PTA-2（女性ユーザに適用される）の価格内容を比較すると、PTA-1の価格内容に示される価格が、PTA-2の価格内容に示される価格の2倍に設定されている。例えば、UCPAの「利用内容11」に対応するPTA-1の「価格内容11」が”2000円”とされているのに対し、同様にUCPAの「利用内容11」に対応するPTA-2の「価格内容21」は”1000円”とされている。同様に、PTA-1の「価格内容12」乃至「価格内容14」に設定されている価格は、PTA-2の「価格内容22」乃至「価格内容24」に設定されている価格に2倍とされている。すなわち、この例の場合、コンテンツAは、女性のユーザがより低価格で利用できるコンテンツとされている。

【0096】

図19は、図9（B）のUCPBに対応して作成された、2つのPTB-1およびPTB-2を表している。図19（A）のPTB-1には、コンテンツAのID、コンテンツプロバイダ2のID、UCPBのID、UCPBの有効期限、サービスプロバイダ3のID、PTB-1のID、PTB-1の有効期限、価格条件30、2通りの価格内容31、32などが含まれている。

【0097】

PTB-1の「価格条件30」の「ユーザ条件30」には”条件なし”が設定され、「機器条件30」には、機器が従機器であることを条件とする情報（”従機器”）が設定されている。すなわち、PTB-1は、コンテンツAが従機器において利用される場合にのみ選択可能となる。なお、従機器とは、自分自身が、所定のコンテンツを購入するための処理や、課金を決済する処理などを行うことができない機器を意味する。

【0098】

PTB-1の「価格条件30」の「ユーザ条件30」および「機器条件30」にも、実際は、図20（A）に示すように、各コードのコード値が設定されている。「ユーザ条件30」には、”条件なし”を意味する0000hのサービスコー

ド(図12(A))が、この場合何ら意味を持たないFFFFFFhのバリューコードが、そして”無条件”を意味する00hのコンディションコード(図12(B))が設定されている。「機器条件30」は、”従機器”とされているので、”機器に関し条件有り”を意味する00xxhのサービスコードが、このとき”数値100”を示す000064hのバリューコードが、そして”<(小さい)”を意味する03hのコンディションコードが設定されている。この例の場合、従機器には、100番より小さい機器番号が設定されているので、このようなコード値が設定される。

【0099】

PTB-1の「価格内容31」の”100円”は、UCPB(図9(B))の「利用内容21」の「形式21」が”Pay Per Play4”とされているので、4回の再生を行う場合の料金を示し、「価格内容32」の”300円”は、UCPBの「利用内容22」の「形式22」が”Pay Per Copy2”とされているので、2回の複製を行う場合の料金を示している。

【0100】

UCPBに対応して作成された、もう一方のPTB-2には、図19(B)に示すように、コンテンツAのID、コンテンツプロバイダ2のID、UCPBのID、UCPB、サービスプロバイダ3のID、PTB-2のID、PTB-2の有効期限、価格条件40、および2通りの価格内容41、42などが含まれている。

【0101】

PTB-2の「価格条件40」の「ユーザ条件40」には”条件なし”が設定され、その「機器条件40」には、機器が主機器であることを条件とする情報(”主機器”)が設定されている。すなわち、PTB-2は、主機器においてコンテンツが利用される場合にのみ選択可能となる。なお、主機器とは、自分自身が、所定のコンテンツを購入するための処理や、課金を決済する処理などを行うことができる機器を意味する。

【0102】

PTB-2の「価格条件40」の「ユーザ条件40」および「機器条件40」にも、実際は、図20(B)に示すように、各コードのコード値が設定されている

。「価格条件 4 0」の「ユーザ条件 4 0」には、”条件なし”を意味する 0 0 0 0 h のサービスコード（図 1 2（A））が、この場合何ら意味を持たない F F F F F F h のバリューコードが、そして”無条件”を意味する 0 0 h のコンディションコード（1 5（B））が設定されている。「機器条件 4 0」には、”機器に関し条件有り”を意味する 0 0 x x h のサービスコードが、このとき”数値 1 0 0”を示す 0 0 0 0 6 4 h のバリューコードが、そして”=>（以上）”を意味する 0 6 h のコンディションコードが設定されている。この例の場合、主機器には、1 0 0 番以上の機器番号が設定されているので、このようなコード値が設定される。

【0 1 0 3】

PTB - 2 の「価格内容 4 1」および「価格内容 4 2」のそれぞれに示される価格は、UCPB の「利用内容 2 1」の「形式 2 1」および「利用内容 2 2」の「形式 2 2」のそれぞれに示される利用形式でコンテンツ A を利用する場合の料金を示している。

【0 1 0 4】

ここで、PTB - 1（従機器に適用される）の価格内容と PTB - 2（主機器に適用される）の価格内容を比較すると、PTB - 1 の価格内容は、PTB - 2 の価格内容の 2 倍に設定されている。例えば、PTB - 1 の「価格内容 3 1」が”1 0 0 円”とされているのに対し、PTB - 2 の「価格内容 4 1」は 5 0 円とされており、「価格内容 3 2」が”3 0 0 円”とされているのに対して、「価格内容 4 2」は”1 5 0 円”とされている。

【0 1 0 5】

図 1 6 に戻り、ポリシー記憶部 4 3 は、コンテンツプロバイダ 2 から供給された、コンテンツの UCP を記憶し、セキュアコンテナ作成部 4 4 に供給する。

【0 1 0 6】

セキュアコンテナ作成部 4 4 は、例えば、図 2 1 に示すような、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、UCPA, B、コンテンツプロバイダ 2 の署名、PT A - 1, A - 2, B - 1, B - 2、およびサービスプロバイダ 3 の署名からなる

サービスプロバイダセキュアコンテナを作成する。

【0107】

セキュアコンテナ作成部44はまた、作成したサービスプロバイダセキュアコンテナを、図22に示すような、証明書のバージョン番号、認証局がサービスプロバイダ3に対し割り付ける証明書の通し番号、署名に用いたアルゴリズムおよびパラメータ、認証局の名前、証明書の有効期限、サービスプロバイダ3の名前、サービスプロバイダ3の公開鍵K_{psp}、並びに署名より構成されるサービスプロバイダの証明書を付して、ユーザホームネットワーク5に供給する。

【0108】

図16に、再び戻り、相互認証部45は、コンテンツプロバイダ2からコンテンツプロバイダセキュアコンテナの供給を受け取るのに先立ち、コンテンツプロバイダ2と相互認証する。相互認証部45また、ユーザホームネットワーク5へのサービスプロバイダセキュアコンテナの送信に先立ち、ユーザホームネットワーク5と相互認証するが、このサービスプロバイダ3とユーザホームネットワーク5との相互認証は、例えば、ネットワーク4が衛星通信である場合、実行されない。なお、この例の場合、コンテンツプロバイダセキュアコンテナおよびサービスプロバイダセキュアコンテナには、特に、秘密情報が含まれていないので、サービスプロバイダ3は、コンテンツプロバイダ2およびユーザホームネットワーク5と相互認証を行わなくてもよい。

【0109】

図23は、ユーザホームネットワーク5を構成するレシーバ51の構成例を表している。レシーバ51は、通信部61、SAM62、外部記憶部63、伸張部64、通信部65、インタフェース66、表示制御部67、および入力制御部68より構成される、HDD52に接続される据え置き型の機器である。

【0110】

レシーバ51の通信部61は、ネットワーク4を介してサービスプロバイダ3、またはEMDサービスセンタ1と通信し、所定の情報を受信し、または送信する。

【0111】

SAM 6 2 は、相互認証モジュール 7 1、課金処理モジュール 7 2、記憶モジュール 7 3、復号/暗号化モジュール 7 4、およびデータ検査モジュール 7 5 からなるが、シングルチップの暗号処理専用 IC で構成され、多層構造を有し、その内部のメモリセルはアルミニウム層等のダミー層に挟まれ、また、動作する電圧または周波数の幅が狭い等、外部から不正にデータが読み出し難い特性（耐タンパ性）を有している。

【0112】

SAM 6 2 の相互認証モジュール 7 1 は、記憶モジュール 7 3 に記憶されている、図 2 4 に示す SAM 6 2 の証明書を、相互認証相手に送信し、相互認証を実行し、これにより、認証相手と共有することとなった一時鍵 K_{temp} （セッション鍵）を復号/暗号化モジュール 7 4 に供給する。SAM の証明書には、コンテンツプロバイダ 2 の証明書（図 1 5）およびサービスプロバイダ 3 の証明書（図 2 2）に含まれている情報に対応する情報が含まれているので、その説明は省略する。

【0113】

課金処理モジュール 7 2 は、選択された UCP の利用内容に基づいて、UCS および課金情報を作成する。図 2 5 は、図 9（A）に示した UCPA の利用内容 1 1 と、図 1 7（A）に示した PTA-1 の価格内容 1 1 に基づいて作成された UCSA を表している。UCS には、図 2 5 に示されるように、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「サービスプロバイダの ID」、「PT の ID」、「PT の有効期限」、「UCS の ID」、「SAM の ID」、「ユーザの ID」、「利用内容」、および「利用履歴」の各項目に対応する所定の情報が設定される。

【0114】

UCS の、「コンテンツの ID」、「コンテンツプロバイダの ID」、「UCP の ID」、「UCP の有効期限」、「サービスプロバイダの ID」、「PT の ID」、および「PT の有効期限」の各項目には、PT の、それらに対応する項目の情報が設定される。すなわち、図 2 5 の UCSA の、「コンテンツの ID」には、コンテンツ A の ID が、「コンテンツプロバイダの ID」には、コンテンツプロバイダ 2 の ID が、「UCP の ID

」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「PTのID」には、PTA-1のIDが、そして「PTの有効期限」には、PTA-1の有効期限が、それぞれ設定されている。

【0115】

「UCSのID」には、UCSに割り当てられた所定のIDが設定され、UCSAの「UCSのID」には、UCSAのIDが設定されている。「SAMのID」には、機器のSAMのIDが設定され、UCSAの「SAMのID」には、レシーバ51のSAM62のIDが設定されている。「ユーザのID」には、コンテンツを利用するユーザのIDが設定され、UCSAの「ユーザのID」には、レシーバ51のユーザのIDが設定されている。

【0116】

「利用内容」は、「ID」、「形式」、「パラメータ」、および「管理移動状態情報」の各項目からなり、そのうち「ID」、「形式」、および「パラメータ」の項目には、選択されたUCPの「利用内容」の、それらに対応する項目の情報が設定される。すなわち、UCSAの「ID」には、UCPAの「利用内容11」の「ID11」に設定されている情報（利用内容11のID）が、「形式」には、「利用内容11」の「形式11」に設定されている”買い取り再生”が、「パラメータ」には、「利用内容11」の「パラメータ11」に設定されている情報（”買い取り再生”に対応する情報）が設定されている。

【0117】

「利用内容」の「管理移動状態情報」には、選択されたUCPの「管理移動許可情報」に”可”が設定されている場合（管理移動が行える場合）、管理移動元の機器（コンテンツを購入した機器）と管理移動先の機器のそれぞれのIDが設定されるようになされている。なお、コンテンツの管理移動が行われていない状態においては、管理移動元の機器のIDが、管理移動先の機器のIDとしても設定される。一方、UCPの「管理移動許可情報」に、”不可”が設定されている場合、「管理移動状態情報」には”不可”が設定される。すなわち、この場合、コンテンツの管理移動は行われず（許可されない）。UCSAの「管理移動状態情報」には、UCPAの「利用内容11」の「管理移動許可情報11」に”可”が設定されて

おり、また、このとき、コンテンツAは管理移動されていないので、SAM 6 2 のIDが、管理移動元の機器のIDおよび管理移動先の機器のIDとして設定されている。

【0118】

「利用履歴」には、同一のコンテンツに対する利用形式の履歴が設定される。UCSAの「利用履歴」には、“買い取り再生”を示す情報のみが記憶されているが、例えば、レシーバ5 1において、コンテンツAが以前に利用されていた場合、そのときの利用形式も記憶される。

【0119】

なお、上述したUCSにおいては、「UCPの有効期限」および「PTの有効期限」が設けられているがそれらをUCSに設定しないようにすることもできる。また、上述したUCSにおいて、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

【0120】

作成されたUCSは、レシーバ5 1の復号／暗号化モジュール7 4の復号化ユニット9 1から供給されるコンテンツ鍵K c o（保存用鍵K s a v eで暗号化されている）とともに、外部記憶部6 3に送信され、その利用情報記憶部6 3 Aに記憶される。外部記憶部6 3の利用情報記憶部6 3 Aは、図2 6に示すように、M個のブロックBP-1乃至BP-Mに分割され（例えば、1メガバイト毎に分割され）、各ブロックBPが、N個の利用情報用メモリ領域RP-1乃至RP-Nに分割されている。SAM 6 2から供給されるコンテンツ鍵K c o（保存用鍵K s a v eで暗号化されている）およびUCSは、利用情報用記憶部6 3 Aの所定のブロックBPの利用情報用メモリ領域RPに、対応して記憶される。

【0121】

図2 6の例では、ブロックBP-1の利用情報用メモリ領域RP-3に、図2 5に示したUCSAとコンテンツ鍵K c o A（保存用鍵K s a v eで暗号化されてい

る)が対応して記憶されている。ブロックBP-1の利用情報用メモリ領域RP-1, RP-2には、他のコンテンツ鍵Kco1, Kco2(それぞれ保存用鍵Ksaveで暗号化されている)およびUCS1, 2がそれぞれ記憶されている。ブロックBP-1の利用情報用メモリ領域RP-4(図示せず)乃至RP-N、およびブロックBP-2(図示せず)乃至BP-Mには、この場合、コンテンツ鍵KcoおよびUCSは記憶されておらず、空いていることを示す所定の初期情報が記憶されている。なお、利用情報用メモリ領域RPに記憶されるコンテンツ鍵Kco(保存用鍵Ksaveで暗号化されている)およびUCSを、個々に区別する必要がない場合、まとめて、利用情報と称する。

【0122】

図27は、図25に示したUCSAと同時に作成された課金情報Aを表している。課金情報は、図27に示されるように、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、「利用内容」、および「課金履歴」の各項目に対応する所定の情報が設定される。

【0123】

課金情報の、「コンテンツのID」、「コンテンツプロバイダのID」、「UCPのID」、「UCPの有効期限」、「サービスプロバイダのID」、「PTのID」、「PTの有効期限」、「UCSのID」、「SAMのID」、「ユーザのID」、および「利用内容」には、UCSの、それらに対応する項目の情報が、それぞれ設定される。すなわち、図27の課金情報Aの、「コンテンツのID」には、コンテンツAのIDが、「コンテンツプロバイダのID」には、コンテンツプロバイダ2のIDが、「UCPのID」には、UCPAのIDが、「UCPの有効期限」には、UCPAの有効期限が、「サービスプロバイダのID」には、サービスプロバイダ3のIDが、「PTのID」には、PTA-1のIDが、「PTの有効期限」には、PTA-1の有効期限が、「UCSのID」には、UCSAのIDが、「SAMのID」には、SAM62のIDが、「ユーザのID」には、ユーザFのIDが、そして「利用内容」には、UCSAの「利用内容11」の内容が、それぞれ設定されている。

【0124】

課金情報の「課金履歴」には、機器において計上された課金の合計額を示す情報が設定される。課金情報Aの「課金履歴」には、レシーバ51において計上された課金の合計額が設定されている。

【0125】

なお、上述した課金情報においては、「UCPの有効期限」および「PTの有効期限」が設けられているが、それらを課金情報に設定しないようにすることもできる。また、上述した課金情報においては、「コンテンツプロバイダのID」が設けられているが、UCPのIDがユニークで、これにより、コンテンツプロバイダを特定することができる場合、それを設けないようにすることもできる。また「サービスプロバイダのID」も同様に、PTのIDがユニークで、これにより、サービスプロバイダを特定することができる場合、それを設けないようにすることもできる。

【0126】

図23に戻り、記憶モジュール73には、図28に示すように、SAM62の公開鍵K_{pu}、SAM62の秘密鍵K_{su}、EMDサービスセンタ1の公開鍵K_{pesc}、認証局の公開鍵K_{pca}、保存用鍵K_{save}、3月分の配送用鍵K_dなどの各種鍵、SAM62の証明書、課金情報、基準情報51、およびM個の検査値HP-1乃至HP-Mなどが記憶されている。

【0127】

記憶モジュール73に記憶される検査値HP-1は、外部記憶部63の利用情報記憶部63AのブロックBP-1に記憶されているデータの全体にハッシュ関数が適用されて算出されたハッシュ値である。検査値HP-2乃至HP-Mも、検査値HP-1と同様に、外部記憶部63の、対応するブロックBP-2乃至BP-Mのそれぞれに記憶されているデータのハッシュ値である。

【0128】

図29は、記憶モジュール73に記憶されている基準情報51を表している。基準情報には、「SAMのID」、「機器番号」、「決済ID」、「課金の上限額」、「決済ユーザ情報」、「従属ユーザ情報」、および「利用ポイント情報」の各項

目に設定される所定情報などが含まれている。

【0129】

基準情報51には、SAM62のID、SAM62の機器番号（100番）、ユーザの決済ID、ユーザの決済ユーザ情報（ユーザの一般情報（氏名、住所、電話番号、決済機関情報、生年月日、年齢、性別）、ユーザのID、およびユーザのパスワード）、および所定の利用ポイント情報が設定されている。

【0130】

「課金の上限額」には、機器がEMDシステムに正式登録されている状態と仮登録されている状態で、それぞれ異なる課金の上限額が設定される。基準情報51の「課金の上限額」には、レシーバ51が正式登録されているので、正式登録されている状態における課金の上限額を示す情報（”正式登録時の上限額”）が設定されている。

【0131】

図23に戻り、SAM62の復号／暗号化モジュール74は、復号ユニット91、乱数発生ユニット92、および暗号化ユニット93から構成される。復号ユニット91は、暗号化されたコンテンツ鍵Kc0を配送用鍵Kdで復号し、暗号化ユニット93に出力する。乱数発生ユニット92は、必要に応じて（例えば、相互認証時に）、所定の桁数の乱数を発生し、必要に応じて一時鍵Ktempを生成し、暗号化ユニット93に出力する。

【0132】

暗号化ユニット93は、復号されたコンテンツ鍵Kc0を、再度、記憶モジュール73に保持されている保存用鍵Ksaveで暗号化する。暗号化されたコンテンツ鍵Kc0は、外部記憶部63に供給される。暗号化ユニット93は、コンテンツ鍵Kc0を伸張部64に送信するとき、コンテンツ鍵Kc0を乱数発生ユニット92で生成した一時鍵Ktempで暗号化する。

【0133】

データ検査モジュール75は、記憶モジュール73に記憶されている検査値HPと、外部記憶部63の利用情報記憶部63Aの、対応するブロックBPのデータのハッシュ値を比較し、ブロックBPのデータが改竄されていないか否かを検査

する。

伸張部 64 は、相互認証モジュール 101、復号モジュール 102、復号モジュール 103、伸張モジュール 104、およびウォーターマーク付加モジュール 105 から構成される。相互認証モジュール 101 は、SAM 62 と相互認証し、一時鍵 *Ktemp* を復号モジュール 102 に出力する。復号モジュール 102 は、一時鍵 *Ktemp* で暗号化されたコンテンツ鍵 *Kco* を一時鍵 *Ktemp* で復号し、復号モジュール 103 に出力する。復号モジュール 103 は、HDD 52 に記録されたコンテンツをコンテンツ鍵 *Kco* で復号し、伸張モジュール 104 に出力する。伸張モジュール 104 は、復号されたコンテンツを、更に ATRAC2 等の方式で伸張し、ウォーターマーク付加モジュール 105 に出力する。ウォーターマーク付加モジュール 105 は、コンテンツにレシーバ 51 を特定するための情報（例えば、SAM 62 の ID）のウォーターマーク（電子透かし）を挿入し、図示せぬスピーカに出力し、音楽を再生する。

【0134】

通信部 65 は、ユーザホームネットワーク 5 のレシーバ 201 との通信処理を行う。インターフェース 66 は、SAM 62 および伸張部 64 からの信号を所定の形式に変更し、HDD 52 に出力し、また、HDD 52 からの信号を所定の形式に変更し、SAM 62 および伸張部 64 に出力する。

【0135】

表示制御部 67 は、表示部（図示せず）への出力を制御する。入力制御部 68 は、各種ボタンなどから構成される操作部（図示せず）からの入力を制御する。

【0136】

HDD 52 は、サービスプロバイダ 3 から供給されたコンテンツなどを記憶する他、図 30 に示すような登録リストを記憶している。この登録リストは、表形式に情報が記憶されているリスト部、および登録リストを保持する機器についての所定の情報が記憶されている対象 SAM 情報部より構成されている。

【0137】

対象 SAM 情報部には、この登録リストを保有する機器の SAMID、この例の場合、レシーバ 51 の SAM 62 の ID が（「対象 SAMID」の欄に）記憶されている。対象 SA

M情報部にはまた、この登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ51には、レシーバ201の1機の機器が接続されているので、自分自身を含む合計値2が（「接続されている機器数」の欄に）記憶されている。

【0138】

リスト部は、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、「状態フラグ」、「公開鍵」、および「署名」の9個の項目から構成され、この例の場合、レシーバ51の登録条件、レシーバ201の登録条件として、それぞれの項目に所定の情報が記憶されている。

【0139】

「SAMID」には、機器のSAMのIDが記憶される。この例の場合、レシーバ51のSAM62のID、およびレシーバ201のSAM212のIDが記憶されている。「ユーザID」には、対応する機器のユーザのユーザIDが記憶される。

【0140】

「購入処理」には、機器が、コンテンツを購入するための処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツを購入するための処理を行うことができるようになされているので、それぞれに対応する「購入処理」には、“可”が記憶されている。

【0141】

「課金処理」には、機器が、EMDサービスセンタ1との間で、課金処理を行うことができるか否かを示す情報（“可”または“不可”）が記憶される。この例の場合、レシーバ51のみが、課金処理を行うことができ、レシーバ201はその処理を行うことができないようになされているので、レシーバ51に対応する「課金処理」には、“可”が記憶され、レシーバ201に対応する「課金処理」には、“不可”が記憶されている。

【0142】

「課金機器」には、機器において計上された課金を決済する処理を行う機器の

SAMのIDが記憶される。この例の場合、レシーバ51（SAM62）は、自分自身の課金を自分自身で決済することができるので、その対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。レシーバ51はまた、自分自身の課金を決済することができないレシーバ201に代わり、その課金を決済するようになされているので、レシーバ201に対応する「課金機器」には、レシーバ51のSAM62のIDが記憶されている。

【0143】

「コンテンツ供給機器」には、機器が、コンテンツの供給をサービスプロバイダ3からではなく、接続される他の機器から受ける場合、コンテンツを供給することができる機器のSAMのIDが記憶される。この例の場合、レシーバ51およびレシーバ201は、コンテンツの供給をサービスプロバイダ3から受けるので、それぞれに対応する「コンテンツ供給機器」には、コンテンツを供給する機器が存在しない旨を示す情報（”なし”）が記憶されている。

【0144】

「状態フラグ」には、機器の動作制限条件が記憶される。何ら制限されていない場合は、その旨を示す情報（”制限なし”）、一定の制限が課せられている場合は、その旨を示す情報（”制限あり”）、また動作が停止される場合には、その旨を示す情報（”停止”）が記憶される。例えば、課金処理が成功しなかった場合、その機器に対応する「状態フラグ」には、”制限あり”が設定される（詳細は後述する）。この例の場合、「状態フラグ」に”制限あり”が設定された機器においては、すでに購入されたコンテンツの再生（解読）処理は実行されるが、新たなコンテンツを購入するための処理は実行されなくなる。すなわち、一定の制限が機器に課せられる。また、コンテンツの不正複製などの違反行為が発覚した場合、「状態フラグ」には、”停止”が設定され、機器の動作が停止される。これにより、その機器はEMDシステムからのサービスを、一切受けることができなくなる。

【0145】

この例の場合、レシーバ51およびレシーバ201に対しては、何ら制限が課せられていないものとし、それぞれに対応する「状態フラグ」には、”なし”が

設定されている。なお、「状態フラグ」に設定される、“制限あり”および“停止”など、動作を制限するための情報を、個々に区別する必要がない場合、まとめて、動作制限情報と称する。

【0146】

「登録条件署名」には、各登録条件として、それぞれ、「SAMID」、「ユーザID」、「購入処理」、「課金処理」、「課金機器」、「コンテンツ供給機器」、および「状態フラグ」に記憶されている情報に対するEMDサービスセンタ1による署名が記憶されている。「登録リスト署名」には、登録リストに設定されているデータの全体に対する署名が記憶されている。

【0147】

図31は、レシーバ201の構成例を表している。レシーバ201の通信部211乃至入力制御部218は、レシーバ51の通信部61乃至入力制御部68と同様の機能を有しているので、その詳細な説明は適宜省略する。

【0148】

HDD202には、購入したコンテンツの他、図32に示すような、レシーバ201の登録リストが記憶されている。この登録リストの対象SAM情報部には、レシーバ201のSAM210のID、その登録リストの有効期限、バージョン番号、接続されている機器の数（この例では、レシーバ201には、レシーバ51の1機が接続され、自分自身を含めた合計数2）が記憶されている。リスト部には、図30のレシーバ51の登録リストのリスト部と同様の情報が記憶されている。

【0149】

次に、EMDシステムの処理について、図33のフローチャートを参照して説明するが、ここでは、コンテンツプロバイダ2に保持されているコンテンツAが、サービスプロバイダ3を介して、ユーザホームネットワーク5のレシーバ51に供給され、利用される場合を例として説明する。

【0150】

ステップS11において、配送用鍵Kdが、EMDサービスセンタ1からコンテンツプロバイダ2に供給される処理が行われる。この処理の詳細は、図34のフローチャートに示されている。すなわち、ステップS31において、EMDサービ

センタ 1 の相互認証部 17 (図 3) は、コンテンツプロバイダ 2 の相互認証部 39 (図 8) と相互認証し、コンテンツプロバイダ 2 が、正当なプロバイダであることが確認した後、EMD サービスセンタ 1 のコンテンツプロバイダ管理部 12 は、鍵サーバ 14 から供給された配送用鍵 K_d をコンテンツプロバイダ 2 に送信する。なお、相互認証処理の詳細は、図 35 乃至図 37 を参照して後述する。

【0151】

次に、ステップ S32 において、コンテンツプロバイダ 2 の暗号化部 36 は、EMD サービスセンタ 1 から送信された配送用鍵 K_d を受信し、ステップ S33 において、記憶する。

【0152】

このように、コンテンツプロバイダ 2 の暗号化部 36 が、配送用鍵 K_d を記憶したとき、処理は終了し、図 33 のステップ S12 に進む。ここで、ステップ S12 の処理の説明の前に、図 34 のステップ S31 における相互認証処理 (なりすましがいないことを確認する処理) について、1 つの共通鍵を用いる場合 (図 35)、2 つの共通鍵を用いる場合 (図 36)、および公開鍵暗号を用いる場合 (図 37) を例として説明する。

【0153】

図 35 は、1 つの共通鍵で、共通鍵暗号である DES を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S41 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R_1 を生成する (乱数生成部 35 が生成するようにしてもよい)。ステップ S42 において、コンテンツプロバイダ 2 の相互認証部 39 は、DES を用いて乱数 R_1 を、予め記憶している共通鍵 K_c で暗号化する (暗号化部 36 で暗号化するようにしてもよい)。ステップ S43 において、コンテンツプロバイダ 2 の相互認証部 39 は、暗号化された乱数 R_1 を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0154】

ステップ S44 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R_1 を予め記憶している共通鍵 K_c で復号する。ステップ S45 において

、EMDサービスセンタ1の相互認証部17は、32ビットの乱数 R_2 を生成する。ステップS46において、EMDサービスセンタ1の相互認証部17は、復号した64ビットの乱数 R_1 の下位32ビットを乱数 R_2 で入れ替え、接続 $R_{1H} \parallel R_2$ を生成する。なお、ここで R_{iH} は、 R_i の上位ビットを表し、 $A \parallel B$ は、AとBの接続（nビットのAの下位に、mビットのBを結合して、 $(n+m)$ ビットとしたもの）を表す。ステップS47において、EMDサービスセンタ1の相互認証部17は、DESを用いて $R_{1H} \parallel R_2$ を共通鍵 K_c で暗号化する。ステップS48において、EMDサービスセンタ1の相互認証部17は、暗号化した $R_{1H} \parallel R_2$ をコンテンツプロバイダ2に送信する。

【0155】

ステップS49において、コンテンツプロバイダ2の相互認証部39は、受信した $R_{1H} \parallel R_2$ を共通鍵 K_c で復号する。ステップS50において、コンテンツプロバイダ2の相互認証部39は、復号した $R_{1H} \parallel R_2$ の上位32ビット R_{1H} を調べ、ステップS41で生成した、乱数 R_1 の上位32ビット R_{1H} と一致すれば、EMDサービスセンタ1が正当なセンタであることを認証する。生成した乱数 R_{1H} と、受信した R_{1H} が一致しないとき、処理は終了される。両者が一致するとき、ステップS51において、コンテンツプロバイダ2の相互認証部39は、32ビットの乱数 R_3 を生成する。ステップS52において、コンテンツプロバイダ2の相互認証部39は、受信し、復号した32ビットの乱数 R_2 を上位に設定し、生成した乱数 R_3 をその下位に設定し、接続 $R_2 \parallel R_3$ とする。ステップS53において、コンテンツプロバイダ2の相互認証部39は、DESを用いて接続 $R_2 \parallel R_3$ を共通鍵 K_c で暗号化する。ステップS54において、コンテンツプロバイダ2の相互認証部39は、暗号化された接続 $R_2 \parallel R_3$ をEMDサービスセンタ1の相互認証部17に送信する。

【0156】

ステップS55において、EMDサービスセンタ1の相互認証部17は、受信した接続 $R_2 \parallel R_3$ を共通鍵 K_c で復号する。ステップS56において、EMDサービスセンタ1の相互認証部17は、復号した接続 $R_2 \parallel R_3$ の上位32ビットを調べ、乱数 R_2 と一致すれば、コンテンツプロバイダ2を正当なプロバイダとして

認証し、一致しなければ、不正なプロバイダとして、処理を終了する。

【0157】

図36は、2つの共通鍵 K_{c1} 、 K_{c2} で、共通鍵暗号であるDESを用いる、コンテンツプロバイダ2の相互認証部39とEMDサービスセンタ1の相互認証部17との相互認証の動作を説明するフローチャートである。ステップS61において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数 R_1 を生成する。ステップS62において、コンテンツプロバイダ2の相互認証部39は、DESを用いて乱数 R_1 を予め記憶している共通鍵 K_{c1} で暗号化する。ステップS63において、コンテンツプロバイダ2の相互認証部39は、暗号化された乱数 R_1 をEMDサービスセンタ1に送信する。

【0158】

ステップS64において、EMDサービスセンタ1の相互認証部17は、受信した乱数 R_1 を予め記憶している共通鍵 K_{c1} で復号する。ステップS65において、EMDサービスセンタ1の相互認証部17は、乱数 R_1 を予め記憶している共通鍵 K_{c2} で暗号化する。ステップS66において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数 R_2 を生成する。ステップS67において、EMDサービスセンタ1の相互認証部17は、乱数 R_2 を共通鍵 K_{c2} で暗号化する。ステップS68において、EMDサービスセンタ1の相互認証部17は、暗号化された乱数 R_1 および乱数 R_2 をコンテンツプロバイダ2の相互認証部39に送信する。

【0159】

ステップS69において、コンテンツプロバイダ2の相互認証部39は、受信した乱数 R_1 および乱数 R_2 を予め記憶している共通鍵 K_{c2} で復号する。ステップS70において、コンテンツプロバイダ2の相互認証部39は、復号した乱数 R_1 を調べ、ステップS61で生成した乱数 R_1 （暗号化する前の乱数 R_1 ）と一致すれば、EMDサービスセンタ1を適正なセンタとして認証し、一致しなければ、不正なセンタであるとして、処理を終了する。ステップS71において、コンテンツプロバイダ2の相互認証部39は、復号して得た乱数 R_2 を共通鍵 K_{c1} で暗号化する。ステップS72において、コンテンツプロバイダ2の相互認

証部 39 は、暗号化された乱数 R_2 を EMD サービスセンタ 1 に送信する。

【0160】

ステップ S73 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した乱数 R_2 を共通鍵 K_{c1} で復号する。ステップ S74 において、EMD サービスセンタ 1 の相互認証部 17 は、復号した乱数 R_2 が、ステップ S66 で生成した乱数 R_2 (暗号化する前の乱数 R_2) と一致すれば、コンテンツプロバイダ 2 を適正なプロバイダとして認証し、一致しなければ、不正なプロバイダであるとして処理を終了する。

【0161】

図 37 は、公開鍵暗号である、160 ビット長の楕円曲線暗号を用いる、コンテンツプロバイダ 2 の相互認証部 39 と EMD サービスセンタ 1 の相互認証部 17 との相互認証の動作を説明するフローチャートである。ステップ S81 において、コンテンツプロバイダ 2 の相互認証部 39 は、64 ビットの乱数 R_1 を生成する。ステップ S82 において、コンテンツプロバイダ 2 の相互認証部 39 は、自分自身の公開鍵 K_{pcp} を含む証明書 (認証局から予め取得しておいたもの) と、乱数 R_1 を EMD サービスセンタ 1 の相互認証部 17 に送信する。

【0162】

ステップ S83 において、EMD サービスセンタ 1 の相互認証部 17 は、受信した証明書の署名 (認証局の秘密鍵 K_{sca} で暗号化されている) を、予め取得しておいた認証局の公開鍵 K_{pca} で復号し、コンテンツプロバイダ 2 の公開鍵 K_{pcp} とコンテンツプロバイダ 2 の名前のハッシュ値を取り出すとともに、証明書に平文のまま格納されているコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前を取り出す。証明書が認証局が発行した適正なものであれば、証明書の署名を復号することが可能であり、復号して得られた公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前のハッシュ値は、平文のまま証明書に格納されていたコンテンツプロバイダ 2 の公開鍵 K_{pcp} およびコンテンツプロバイダ 2 の名前にハッシュ関数を適用して得られたハッシュ値と一致する。これにより、公開鍵 K_{pcp} が改竄されたものでない適正なものであることが認証される。署名を復号出来なかったり、できたとしてもハッシュ値が一致しな

いときには、適正な公開鍵でないか、適正なプロバイダでないことになる。この時処理は終了される。

【0163】

適正な認証結果が得られたとき、ステップS84において、EMDサービスセンタ1の相互認証部17は、64ビットの乱数R2を生成する。ステップS85において、EMDサービスセンタ1の相互認証部17は、乱数R1および乱数R2の接続 $R1 \parallel R2$ を生成する。ステップS86において、EMDサービスセンタ1の相互認証部17は、接続 $R1 \parallel R2$ を自分自身の秘密鍵 K_{sec} で暗号化する。ステップS87において、EMDサービスセンタ1の相互認証部17は、接続 $R1 \parallel R2$ を、ステップS83で取得したコンテンツプロバイダ2の公開鍵 K_{cp} で暗号化する。ステップS88において、EMDサービスセンタ1の相互認証部17は、秘密鍵 K_{sec} で暗号化された接続 $R1 \parallel R2$ 、公開鍵 K_{cp} で暗号化された接続 $R1 \parallel R2$ 、および自分自身の公開鍵 K_{pe} を含む証明書（認証局から予め取得しておいたもの）をコンテンツプロバイダ2の相互認証部39に送信する。

【0164】

ステップS89において、コンテンツプロバイダ2の相互認証部39は、受信した証明書の署名を予め取得しておいた認証局の公開鍵 K_{ca} で復号し、正しければ証明書から公開鍵 K_{pe} を取り出す。この場合の処理は、ステップS83における場合と同様であるので、その説明は省略する。ステップS90において、コンテンツプロバイダ2の相互認証部39は、EMDサービスセンタ1の秘密鍵 K_{sec} で暗号化されている接続 $R1 \parallel R2$ を、ステップS89で取得した公開鍵 K_{pe} で復号する。ステップS91において、コンテンツプロバイダ2の相互認証部39は、自分自身の公開鍵 K_{cp} で暗号化されている接続 $R1 \parallel R2$ を、自分自身の秘密鍵 K_{sc} で復号する。ステップS92において、コンテンツプロバイダ2の相互認証部39は、ステップS90で復号された接続 $R1 \parallel R2$ と、ステップS91で復号された接続 $R1 \parallel R2$ を比較し、一致すればEMDサービスセンタ1を適正なものとして認証し、一致しなければ、不適正なものとして、処理を終了する。

【0165】

適正な認証結果が得られたとき、ステップS93において、コンテンツプロバイダ2の相互認証部39は、64ビットの乱数R3を生成する。ステップS94において、コンテンツプロバイダ2の相互認証部39は、ステップS90で取得した乱数R2および生成した乱数R3の接続R2 || R3を生成する。ステップS95において、コンテンツプロバイダ2の相互認証部39は、接続R2 || R3を、ステップS89で取得した公開鍵K_{pub}で暗号化する。ステップS96において、コンテンツプロバイダ2の相互認証部39は、暗号化した接続R2 || R3をEMDサービスセンタ1の相互認証部17に送信する。

【0166】

ステップS97において、EMDサービスセンタ1の相互認証部17は、暗号化された接続R2 || R3を自分自身の秘密鍵K_{sec}で復号する。ステップS98において、EMDサービスセンタ1の相互認証部17は、復号した乱数R2が、ステップS84で生成した乱数R2（暗号化する前の乱数R2）と一致すれば、コンテンツプロバイダ2を適正なプロバイダとして認証し、一致しなければ、不適正なプロバイダとして、処理を終了する。

【0167】

以上のように、EMDサービスセンタ1の相互認証部17とコンテンツプロバイダ2の相互認証部39は、相互認証する。相互認証に利用された乱数は、その相互認証に続く処理にだけ有効な一時鍵K_{temp}として利用される。

【0168】

次に、図33のステップS12の処理について説明する。ステップS12においては、コンテンツプロバイダセキュアコンテナが、コンテンツプロバイダ2からサービスプロバイダ3に供給される処理が行われる。その処理の詳細は、図38のフローチャートに示されている。すなわち、ステップS201において、コンテンツプロバイダ2のウォーターマーク付加部32（図8）は、コンテンツサーバ31からコンテンツAを読み出し、コンテンツプロバイダ2を示す所定のウォーターマーク（電子透かし）を挿入し、圧縮部33に供給する。

【0169】

ステップ S 2 0 2 において、コンテンツプロバイダ 2 の圧縮部 3 3 は、ウォーターマークが挿入されたコンテンツ A を ATRAC2 等の所定の方式で圧縮し、暗号化部 3 4 に供給する。ステップ S 2 0 3 において、乱数発生部 3 5 は、コンテンツ鍵 K c o A となる乱数を発生させ、暗号化部 3 4 に供給する。

【0170】

ステップ S 2 0 4 において、コンテンツプロバイダ 2 の暗号化部 3 4 は、DES などの所定の方式で、乱数発生部 3 5 で発生された乱数（コンテンツ鍵 K c o A）を使用して、ウォーターマークが挿入されて圧縮されたコンテンツ A を暗号化する。次に、ステップ S 2 0 5 において、暗号化部 3 6 は、DES などの所定の方式で、EMD サービスセンタ 1 から供給された配送用鍵 K d でコンテンツ鍵 K c o A を暗号化する。

【0171】

ステップ S 2 0 6 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、およびポリシー記憶部 3 7 に記憶されている、コンテンツ A に対応する UCPA, B（図 9）の全体にハッシュ関数を適用してハッシュ値を算出し、自分自身の秘密鍵 K s c p で暗号化する。これにより、図 1 4 に示した署名が作成される。

【0172】

ステップ S 2 0 7 において、コンテンツプロバイダ 2 のセキュアコンテナ作成部 3 8 は、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、UCPA, B（図 9）、およびステップ S 2 0 6 で生成した署名を含んだ、図 1 4 に示したコンテンツプロバイダセキュアコンテナを作成する。

【0173】

ステップ S 2 0 8 において、コンテンツプロバイダ 2 の相互認証部 3 9 は、サービスプロバイダ 3 の相互認証部 4 5（図 1 6）と相互認証する。この認証処理は、図 3 5 乃至図 3 7 を参照して説明した場合と同様であるので、その説明は省略する。ステップ S 2 0 9 において、コンテンツプロバイダ 2 のセキュアコンテ

ナ作成部 38 は、認証局から予め発行された証明書（図 15）を、ステップ S 207 で作成したコンテンツプロバイダセキュアコンテナに付して、サービスプロバイダ 3 に送信する。

【0174】

このようにして、コンテンツプロバイダセキュアコンテナが、サービスプロバイダ 3 に供給されたとき、処理は終了し、図 33 のステップ S 13 に進む。

【0175】

ステップ S 13 において、サービスプロバイダセキュアコンテナが、サービスプロバイダ 3 からユーザホームネットワーク 5（レシーバ 51）に供給される。この処理の詳細は、図 39 のフローチャートに示されている。すなわち、ステップ S 221 において、サービスプロバイダ 3 の値付け部 42（図 16）は、コンテンツプロバイダ 2 から送信されたコンテンツプロバイダセキュアコンテナに付された証明書（図 15）に含まれる署名を確認し、証明書の改竄がなければ、それから、コンテンツプロバイダ 2 の公開鍵 $K_{p\ c\ p}$ を取り出す。証明書の署名の確認は、図 37 のステップ S 83 における処理と同様であるので、その説明は省略する。

【0176】

ステップ S 222 において、サービスプロバイダ 3 の値付け部 42 は、コンテンツプロバイダ 2 から送信されたコンテンツプロバイダセキュアコンテナの署名をコンテンツプロバイダ 2 の公開鍵 $K_{p\ c\ p}$ で復号し、得られたハッシュ値が、コンテンツ A（コンテンツ鍵 $K_{c\ o\ A}$ で暗号化されている）、コンテンツ鍵 $K_{c\ o\ A}$ （配送用鍵 K_d で暗号化されている）、および UCPA、B の全体にハッシュ関数を適用して得られたハッシュ値と一致するか否かを判定し、コンテンツプロバイダセキュアコンテナの改竄がないことを確認する。両者の値が一致しない場合（改竄が発見された場合）は、処理は終了されるが、この例の場合、コンテンツプロバイダセキュアコンテナの改竄はなかったものとし、ステップ S 223 に進む。

【0177】

ステップ S 223 において、サービスプロバイダ 3 の値付け部 42 は、コンテ

ンツプロバイダセキュアコンテナから、コンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、および署名を取り出し、コンテンツサーバ 4 1 に供給する。コンテンツサーバ 4 1 は、それらを記憶する。値付け部 4 2 はまた UCP A、B も、コンテンツプロバイダセキュアコンテナから取り出し、セキュアコンテナ作成部 4 4 に供給する。

【0178】

ステップ S 2 2 4 において、サービスプロバイダ 3 の値付け部 4 2 は、取り出した UCP A、B に基づいて、PTA-1、A-2（図 1 7）、および PTB-1、B-2（図 1 9）を作成し、セキュアコンテナ作成部 4 4 に供給する。

【0179】

ステップ S 2 2 5 において、サービスプロバイダ 3 のセキュアコンテナ作成部 4 4 は、コンテンツサーバ 4 1 から読み出したコンテンツ A（コンテンツ鍵 K c o A で暗号化されている）、コンテンツ鍵 K c o A（配送用鍵 K d で暗号化されている）、およびコンテンツプロバイダ 2 の署名、値付け部 4 2 から供給された、UCP A、B、および PTA-1、A-2、B-1、B-2、並びにその署名から、図 2 1 に示したサービスプロバイダセキュアコンテナを作成する。

【0180】

ステップ S 2 2 6 において、サービスプロバイダ 3 の相互認証部 4 5 は、レシーバ 5 1 の相互認証モジュール 7 1（図 2 3）と相互認証する。この認証処理は、図 3 5 乃至図 3 7 を参照して説明した場合と同様であるので、その説明を省略する。

【0181】

ステップ S 2 2 7 において、サービスプロバイダ 3 のセキュアコンテナ作成部 4 4 は、ステップ S 2 2 5 で作成したサービスプロバイダセキュアコンテナに、サービスプロバイダ 3 の証明書（図 2 2）を付して、ユーザホームネットワーク 5 のレシーバ 5 1 に送信する。

【0182】

このようにして、サービスプロバイダセキュアコンテナが、サービスプロバイ

ダ3からレシーバ51に送信されたとき、処理は終了し、図33のステップS14に進む。

【0183】

ステップS14において、サービスプロバイダ3から送信されたサービスプロバイダセキュアコンテナが、ユーザホームネットワーク5のレシーバ51により受信される。この処理の詳細は、図40のフローチャートに示されている。すなわち、ステップS241において、レシーバ51の相互認証モジュール71（図23）は、通信部61を介して、サービスプロバイダ3の相互認証部45（図16）と相互認証し、相互認証できたとき、通信部61は、相互認証したサービスプロバイダ3-1から、サービスプロバイダセキュアコンテナ（図21）を受信する。相互認証できなかった場合、処理は終了されるが、この例の場合、相互認証されたものとし、ステップS242に進む。

【0184】

ステップS242において、レシーバ51の通信部61は、ステップS241で相互認証したサービスプロバイダ3から、公開鍵証明書を受信する。

【0185】

ステップS243において、レシーバ51の復号／暗号化モジュール74は、ステップS241で受信したサービスプロバイダセキュアコンテナに含まれる署名を検証し、改竄がなかったか否かを検証する。ここで、改竄が発見された場合、処理は終了するが、この例の場合、改竄が発見されなかったものとし、ステップS244に進む。

【0186】

ステップS244において、レシーバ51の記憶モジュール73に記憶されている基準情報51（図29）が、利用条件を満たすUCPと価格条件を満たすPTが選択され、表示制御部67を介して、図示せず表示部に表示される。ユーザは、表示されたUCPおよびPTの内容を参照して、図示せぬ操作部を操作し、UCPの1つの利用内容を選択する。これにより、入力制御部68は、操作部から入力された、ユーザの操作に対応する信号をSAM62に出力する。

【0187】

この例の場合、レシーバ 5 1 の基準情報 5 1 の「利用ポイント情報」には、利用ポイントが 2 2 2 ポイントであるとされているものとする。すなわち、コンテンツ A に対応して設定された UCP A, B のうち、「利用条件 1 0」の「ユーザ条件 1 0」が” 2 0 0 ポイント以上”とされている、UCP A が選択される。また、基準情報 5 1 の「決済ユーザ情報」には、ユーザは男性とされているので、PTA - 1 (図 1 7 (A)) の「価格条件 1 0」に設定された条件を満たす。その結果、UCP A に対応して作成された PTA - 1, PTA - 2 のうち、PTA - 1 が選択される。結局、UCP A および PTA - 1 の内容が、表示部に表示される。また、この例の場合、これにより、ユーザが、UCP A の利用内容 1 1 (PTA - 1 の価格内容 1 1) を選択したものとする。

【0 1 8 8】

ステップ S 2 4 5 において、レシーバ 5 1 の SAM 6 2 の課金処理モジュール 7 2 は、ステップ S 2 4 4 で選択された、UCP A の「利用内容 1 1」の内容 (PTA - 1 の「価格内容 1 1」の内容) に基づいて、UCSA (図 2 5) および課金情報 A (図 2 7) を作成する。すなわち、この場合、コンテンツ A は、料金が 2 0 0 0 円で買い取り再生される。

【0 1 8 9】

ステップ S 2 4 6 において、サービスプロバイダセキュアコンテナ (図 2 1) に含まれる、コンテンツ A (コンテンツ鍵 K c o A で暗号化されている)、UCP A、PTA - 1, A - 2、およびコンテンツプロバイダ 2 の署名が取り出され、HD D 5 2 に出力され、記憶される。ステップ S 2 4 7 において、復号/暗号化ユニット 7 4 の復号ユニット 9 1 は、サービスプロバイダセキュアコンテナに含まれるコンテンツ鍵 K c o A (配送用鍵 K d で暗号化されている) を、記憶モジュール 7 3 に記憶されている配送用鍵 K d で復号する。

【0 1 9 0】

ステップ S 2 4 8 において、復号/暗号化ユニット 7 4 の暗号化ユニット 9 3 は、ステップ S 2 4 7 で復号されたコンテンツ鍵 K c o A を、記憶モジュール 7 3 に記憶されている保存用鍵 K s a v e で暗号化する。

【0 1 9 1】

ステップS249において、SAM62のデータ検査モジュール75は、ステップS248で保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSAが対応して記憶される、外部記憶部63の利用情報記憶部63A（図26）のブロックBPを検出する。この例の場合、利用情報記憶部63AのブロックBP-1が検出される。なお、図26の利用情報記憶部63Aにおいて、そのブロックBP-1の利用情報用メモリ領域RP-3にコンテンツ鍵KcoAおよびUCSAが記憶されているように示されているが、この例の場合、この時点において、それらは記憶されておらず、ブロックBP-1の利用情報用メモリ領域RP-3は、空いており、所定の初期情報が記憶されているものとする。

【0192】

ステップS250において、レシーバ51のデータ検査モジュール75は、ステップS249で検出したブロックBP-1のデータ（利用情報用メモリ領域RP-1乃至RP-Nに記憶されている全てのデータ）にハッシュ関数を適用して、ハッシュ値を得る。次に、ステップS251において、データ検査モジュール75は、ステップS250で得られたハッシュ値と、記憶モジュール73に記憶されているブロックBP-1に対応する検査値HP-1（図28）とを比較し、一致するか否かを判定し、一致すると判定した場合、そのブロックBP-1のデータは改竄されていないので、ステップS252に進む。

【0193】

ステップS252において、レシーバ51のSAM62は、利用情報（ステップS248で、保存用鍵Ksaveで暗号化されたコンテンツ鍵KcoA、およびステップS245で作成されたUCSA（図25））を、図26に示すように、利用情報記憶部63A（外部記憶部63）のブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。

【0194】

ステップS253において、レシーバ51のデータ検査モジュール75は、ステップS252で利用情報が記憶された利用情報用メモリ領域RP-3が属する、利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用し、

ハッシュ値を算出し、ステップ S 2 5 4 において、記憶モジュール 7 3 に記憶されている検査値 HP-1 に上書きする。ステップ S 2 5 5 において、課金処理モジュール 7 2 は、ステップ S 2 4 5 で作成した課金情報 A を記憶モジュール 7 3 に記憶させ、処理は終了する。

【0 1 9 5】

ステップ S 2 5 1 において、算出されたハッシュ値と検査値 HP-1 とが一致しないと判定された場合、ブロック BP-1 のデータは改竄されているので、手続きは、ステップ S 2 5 6 に進み、データ検査モジュール 7 5 は、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック BP を調べたか否かを判定し、外部記憶部 6 3 の全てのブロック BP を調べていないと判定した場合、ステップ S 2 5 7 に進み、利用情報記憶部 6 3 A の、調べていない（空きを有する他の）ブロック BP を検索し、ステップ S 2 5 0 に戻り、それ以降の処理が実行される。

【0 1 9 6】

ステップ S 2 5 6 において、外部記憶部 6 3 の利用情報記憶部 6 3 A の全てのブロック BP が調べられたと判定された場合、利用情報を記憶できるブロック BP（利用情報用メモリ領域 RP）は存在しないので、処理は終了する。

【0 1 9 7】

このように、サービスプロバイダセキュアコンテナが、レシーバ 5 1 により受信されると、処理は終了し、図 3 3 のステップ S 1 5 に進む。

【0 1 9 8】

ステップ S 1 5 において、供給されたコンテンツ A が、レシーバ 5 1 において利用される。なお、この例の場合、図 4 0 のステップ S 2 2 4 で選択された UCP A の利用内容 1 1 によれば、コンテンツ A は、再生して利用される。そこで、ここでは、コンテンツ A の再生処理について説明する。この再生処理の詳細は、図 4 1 のフローチャートに示されている。

【0 1 9 9】

ステップ S 2 6 1 において、レシーバ 5 1 のデータ検査モジュール 7 5 は、図 4 0 のステップ S 2 5 2 で、コンテンツ鍵 K c o A（保存用鍵 K s a v e で暗号化されている）および UCSA が記憶された利用情報用メモリ領域 RP-3 が属する

、外部記憶部 63 の利用情報記憶部 63A のブロック BP-1 のデータにハッシュ関数を適用してハッシュ値を算出する。

【0200】

ステップ S262 において、レシーバ 51 のデータ検査モジュール 75 は、ステップ S261 において算出したハッシュ値が、図 40 のステップ S253 で算出し、ステップ S254 で記憶モジュール 73 に記憶させたハッシュ値（検査値 HP-1）と一致するか否かを判定し、一致すると判定した場合、ブロック BP-1 のデータは改竄されていないので、ステップ S263 に進む。

【0201】

ステップ S263 において、UCSA（図 25）の「利用内容」の「パラメータ」に示されている情報に基づいて、コンテンツ A が利用可能か否かが判定される。例えば、「利用内容」の「形式」が、「期間制限再生」とされている UCS においては、その「パラメータ」には、その開始期間（時刻）と終了期間（時刻）が記憶されているので、この場合、現在の時刻が、その範囲内にあるか否かが判定される。すなわち、現在時刻が、その範囲内にあるとき、そのコンテンツの利用が可能であると判定され、範囲外にあるとき、利用不可と判定される。また、「利用内容」の「形式」が、所定の回数に限って再生（複製）する利用形式とされている UCS においては、その「パラメータ」には、残された利用可能回数が記憶されている。この場合、「パラメータ」に記憶されている利用可能回数が 0 回でないとき、対応するコンテンツの利用が可能であると判定され、一方、利用可能回数が 0 回であるとき、利用不可と判定される。

【0202】

なお、UCSA の「利用内容」の「形式」は、「買い取り再生」とされているので、この場合、コンテンツ A は、買い取られ、制限なしに再生される。すなわち、UCSA の「利用内容」の「パラメータ」には、コンテンツが利用可能であることを示す情報が設定されている。そのため、この例の場合では、ステップ S263 において、コンテンツ A が利用可能であると判定され、ステップ S264 に進む。

【0203】

ステップS264において、レシーバ51の課金モジュール72は、UCSAを更新する。UCSAには、更新すべき情報は含まれていないが、例えば、「利用内容」の「形式」が所定の回数に限って再生する利用形式とされている場合、その「パラメータ」に記憶されている、再生可能回数が1つだけデクリメントされる。

【0204】

次に、ステップS265において、レシーバ51のSAM62は、ステップS264で更新されたUCSA（実際は、更新されていない）を、外部記憶部63の利用情報記憶部63AのブロックBP-1の利用情報用メモリ領域RP-3に記憶させる。ステップS266において、データ検査モジュール75は、ステップS265でUCSAが記憶された、外部記憶部63の利用情報記憶部63AのブロックBP-1のデータにハッシュ関数を適用して、ハッシュ値を算出し、記憶モジュール73に記憶されている検査値HP-1に上書きする。

【0205】

ステップS267において、SAM62の相互認証モジュール71と、伸張部64の相互認証モジュール101は、相互認証し、SAM62および伸張部64は、一時鍵Ktempを共有する。この認証処理は、図35乃至図37を参照して説明した場合と同様であるので、ここでは説明を省略する。相互認証に用いられる乱数R1、R2、R3、またはその組み合わせが、一時鍵Ktempとして用いられる。

【0206】

ステップS268において、復号/暗号化モジュール74の復号ユニット91は、図40のステップS252で外部記憶部63の利用情報記憶部63AのブロックBP-1（利用情報用メモリ領域RP-3）に記憶されたコンテンツ鍵KcoA（保存用鍵Ksaveで暗号化されている）を、記憶モジュール73に記憶された保存用鍵Ksaveで復号する。

【0207】

次に、ステップS269において、復号/暗号化モジュール74の暗号化ユニット93は、復号されたコンテンツ鍵KcoAを一時鍵Ktempで暗号化する。

。ステップ S 270 において、SAM 62 は、一時鍵 K t e m p で暗号化されたコンテンツ鍵 K c o A を伸張部 64 に送信する。

【0208】

ステップ S 271 において、伸張部 64 の復号モジュール 102 は、コンテンツ鍵 K c o A を一時鍵 K t e m p で復号する。ステップ S 272 において、伸張部 64 は、インタフェース 66 を介して、HDD 52 に記録されたコンテンツ A（コンテンツ鍵 K c o で暗号化されている）を受け取る。ステップ S 273 において、伸張部 64 の復号モジュール 103 は、コンテンツ A（コンテンツ鍵 K c o で暗号化されている）をコンテンツ鍵 K c o A で復号する。

【0209】

ステップ S 274 において、伸張部 64 の伸張モジュール 104 は、復号されたコンテンツ A を ATRAC2 などの所定の方式で伸張する。ステップ S 275 において、伸張部 64 のウォーターマーク付加モジュール 105 は、伸張されたコンテンツ A にレシーバ 51 を特定する所定のウォーターマーク（電子透かし）を挿入する。ステップ S 276 において、コンテンツ A は、図示せぬスピーカなどに出力され、処理は終了する。

【0210】

ステップ S 262 において、ステップ S 261 において算出されたハッシュ値が、レシーバ 51 の記憶モジュール 73 に記憶されたハッシュ値と一致しないと判定された場合、またはステップ S 263 において、コンテンツが利用不可と判定された場合、ステップ S 277 において、SAM 62 は、表示制御部 67 を介して、図示せぬ表示部にエラーメッセージを表示させる等の所定のエラー処理を実行し、処理は終了する。

【0211】

このようにして、レシーバ 51 において、コンテンツ A が再生（利用）されたとき、処理は終了し、図 33 の処理も終了する。

【0212】

次に、レシーバ 51 において計上された課金を決済する場合の処理手順を、図 42 のフローチャートを参照して説明する。なお、この処理は、計上された課金

が所定の上限額（正式登録時の上限額または仮登録時の上限額）を越えた場合、または配送用鍵K dのバージョンが古くなり、例えば、図40のステップS247で、コンテンツ鍵K c o（配送用鍵K dで暗号化されている）を復号することができなくなった場合（サービスプロバイダセキュアコンテナを受信することができなくなった場合）に開始される。

【0213】

ステップS301において、レシーバ51とEMDサービスセンタ1との相互認証が行われる。この相互認証は、図35乃至図37を参照して説明した場合と同様の処理であるので、その説明は省略する。

【0214】

次に、ステップS302において、レシーバ51のSAM62は、EMDサービスセンタ1のユーザ管理部18（図3）に証明書を送信する。ステップS303において、レシーバ51のSAM62は、記憶モジュール73に記憶されている課金情報を、ステップS301でEMDサービスセンタ1と共有した一時鍵K t e m pで暗号化し、配送用鍵K dのバージョン、対応するUCPとPT、並びに登録リストとともに、EMDサービスセンタ1に送信する。

【0215】

ステップS304において、EMDサービスセンタ1のユーザ管理部18は、ステップS303で、レシーバ51から送信された情報を受信し、復号した後、EMDサービスセンタ1のユーザ管理部18が、登録リストの「状態フラグ」に”停止”が設定されるべき不正行為がレシーバ51において存在するか否かを確認する。

【0216】

ステップS305において、EMDサービスセンタ1の課金請求部19は、ステップS303で受信された課金情報を解析し、ユーザ（例えば、ユーザF）の支払い金額を算出する処理等を行う。次に、ステップS306において、ユーザ管理部18は、ステップS305における処理により、決済が成功したか否かを確認する。

【0217】

次に、ステップ S 3 0 7 において、EMDサービスセンタ 1 のユーザ管理部 1 8 は、ステップ S 3 0 4 における確認結果、およびステップ S 3 0 6 における確認結果に基づいて、レシーバ 5 1 の登録条件を設定し、それに署名を付して、レシーバ 5 1 の登録リストを作成する。

【0218】

例えば、ステップ S 3 0 4 で、不正行為が確認された場合、「状態フラグ」には”停止”が設定され、この場合、今後、全ての処理が停止される。すなわち、EMDシステムからのサービスを一切受けることができなくなる。また、ステップ S 3 0 6 で、決済が成功しなかったことが確認された場合、「状態フラグ」には”制限あり”が設定され、この場合、すでに購入したコンテンツを再生する処理は可能とされるが、新たにコンテンツを購入する処理は実行できなくなる。

【0219】

次に、ステップ S 3 0 8 に進み、EMDサービスセンタ 1 のユーザ管理部 1 8 は、最新バージョンの配送用鍵 K d （3 月分の最新バージョンの配送用鍵 K d ）およびステップ S 3 0 7 で作成された登録リストを、一時鍵 K t e m p で暗号化し、レシーバ 5 1 に送信する。

【0220】

ステップ S 3 0 9 において、レシーバ 5 1 の SAM 6 2 は、EMDサービスセンタ 1 から送信された配送用鍵 K d および登録リストを、通信部 6 1 を介して受信し、復号した後、記憶モジュール 7 3 に記憶させる。このとき、記憶モジュール 7 3 に記憶されていた課金情報は消去され、登録リストおよび配送用鍵 K d が更新される。また、このとき、受信された登録リストの登録リスト署名が検証され、登録リストが改竄されていないとが確認される。この署名の確認処理は、図 3 7 のステップ S 8 3 における処理と同様であるので、その説明は省略する。

【0221】

次に、レシーバ 5 1 が、レシーバ 2 0 1 において計上された課金を決済する場合（代理決済する場合）の処理手順を、図 4 3 乃至図 4 5 のフローチャートを参照して説明する。レシーバ 5 1 が、レシーバ 2 0 1 から、代理決済を依頼する所定の信号を受信すると、ステップ S 3 2 1 において、レシーバ 5 1 の相互認証モ

ジュール71は、レシーバ201の相互認証モジュール221と相互認証を行う。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ201のSAM212のIDを取得し、レシーバ201と一時鍵 K_{temp} を共有する。

【0222】

ステップS322において、レシーバ51のSAM62は、HDD52に記憶されている登録リストが改竄されているか否かを判定する。具体的には、登録リストの「登録リスト署名」に記憶されている署名が、公開鍵暗号の公開鍵で復号され、その結果（ハッシュ値）と、その登録リストのデータの全体のハッシュ値とが、等しいか否かが判定される。

【0223】

ステップS322で、登録リストが改竄されていないと判定された場合、ステップS323に進み、レシーバ51のSAM62は、レシーバ201が、代理決済することができる（代理決済すべき）機器であるか否かを判定する。具体的には、ステップS321で取得されたSAM212のIDが、登録リストの「SAMID」に登録され、そしてそれに対応する「課金機器」に自分自身（SAM62）が登録されているか否かが判定される。

【0224】

ステップS323において、この例の場合のように、レシーバ201が代理決済することができる機器であると判定した場合、レシーバ51のSAM62は、ステップS324に進み、課金情報の提供を要求する所定の信号を通信部65を介して、レシーバ201に送信し、ステップS325において、レシーバ201から送信されてきた課金情報を受信する。

【0225】

ステップS326において、レシーバ51は、EMDサービスセンタ1と相互認証する。この相互認証は、図35乃至図37を参照して説明した場合と同様であるので、その説明は省略する。ステップS327において、レシーバ51のSAM62は、ステップS325で受信した課金情報、記憶モジュール73に記憶され

ている配送用鍵K dのバージョン、またHDD 5 2に記憶されている登録リストを、一時鍵K t e m pで暗号化し、EMDサービスセンタ 1 に送信する。

【0226】

ステップS 3 2 8において、EMDサービスセンタ 1 のユーザ管理部 1 8は、レシーバ 5 1から送信された情報を受信し、復号した後、EMDサービスセンタ 1 の監査部 2 1が、登録リストの「状態フラグ」に” 停止” が設定されるべき不正行為が、レシーバ 5 1において存在するか否かを確認する。

【0227】

次に、ステップS 3 2 9において、EMDサービスセンタ 1 のユーザ管理部 1 8は、ステップS 3 2 8での確認結果に基づいて、レシーバ 5 1に不正行為が存在するか否かを判定し、レシーバ 5 1に不正行為が存在しないと判定した場合、ステップS 3 3 0に進む。

【0228】

ステップS 3 3 0において、EMDサービスセンタ 1 の課金請求部 1 9は、ステップS 3 2 8で受信された課金情報を解析し、ユーザの支払い金額を算出する処理等を行う。次に、ステップS 3 3 1において、EMDサービスセンタ 1 のユーザ管理部 1 8は、ステップS 3 3 0における決済の結果に基づいて、レシーバ 5 1およびレシーバ 2 0 1の登録条件を設定し、登録条件署名および登録リスト署名を付して、それぞれの登録リストを作成する。

【0229】

次に、ステップS 3 3 2に進み、EMDサービスセンタ 1 のユーザ管理部 1 8は、最新バージョンの配送用鍵K d、並びにステップS 3 3 1で作成されたレシーバ 5 1の登録リストとレシーバ 2 0 1の登録リストを、一時鍵K t e m pで暗号化して、レシーバ 5 1に送信する。

【0230】

ステップS 3 3 3において、レシーバ 5 1のSAM 6 2は、EMDサービスセンタ 1 から送信された配送用鍵K d、並びにレシーバ 5 1の登録リストとレシーバ 2 0 1の登録リストを受信し、復号すると、ステップS 3 3 4において、レシーバ 5 1の登録リストの、レシーバ 2 0 1のSAM 2 1 2のIDに対応する「状態フラグ」

に、動作制限情報（例えば、“制限あり”または“停止”が）設定されているかを判定し、それが設定されていない場合、ステップS335に進む。

【0231】

ステップS335において、レシーバ51のSAM62は、ステップS325で受信された、レシーバ201からの課金情報を消去し、ステップS336において、配送用鍵Kdおよびレシーバ51の登録リストを更新する。

【0232】

次に、ステップS337において、レシーバ51のSAM62は、レシーバ201に対して、相互認証（図33乃至図35を参照して説明した処理）を行った後、レシーバ201に、レシーバ201の登録リストと配送用鍵Kdを一時鍵Ktempで暗号化して、送信する。

【0233】

ステップS338において、レシーバ201は、レシーバ51から送信されてきたレシーバ201の登録リストおよび配送用鍵Kdを受信し、一時鍵Ktempで復号した後、記憶する（更新）する。

【0234】

ステップS334で、「状態フラグ」に動作制限情報が設定されていると判定された場合、ステップS339に進み、レシーバ51のSAM62は、レシーバ201に対して、所定の処理（REVOKE処理）を実行し、レシーバ201において実行される処理を制限する。

【0235】

ステップS329において、レシーバ51において不正行為が確認された場合、ステップS340に進み、EMDサービスセンタ1は、レシーバ51およびレシーバ201に対応する「状態フラグ」の全てに“停止”を設定し、それぞれの登録リストを作成し、ステップS341において、それらをレシーバ51に送信する。

【0236】

ステップS342において、レシーバ51は、EMDサービスセンタ1から送信

された登録リストを受信し、登録リストを更新する。その後、ステップS339に進み、レシーバ51は、登録リストの「状態フラグ」に設定された動作制限情報に対応する処理を行う。この場合、配送用鍵Kdは、レシーバ51およびレシーバ201には供給されず、レシーバ51およびレシーバ201は、供給されたコンテンツを再生することができなくなり、その結果、EMDシステムにおけるサービスを一切受けることができなくなる。

【0237】

ステップS322において、登録リストが改竄されていると判定された場合、またステップS323において、代理決済することができる機器ではないと判定された場合、処理は終了される。

【0238】

以上のようにして、レシーバ201において計上された課金が、レシーバ51により代理決済させる。

【0239】

図46は、ユーザホームネットワーク5の他の構成例を表している。なお、図中、図1のユーザホームネットワーク5における場合と対応する部分については、同一の符号を付してある。すなわち、レシーバ201に代わり、L個のレシーバ251-1乃至251-L（以下、個々に区別する必要がない場合、単に、レシーバ251と称する。他の装置についても同様である）、およびHDD202に代わり、L個のHDD252-1乃至252-Lが設けられている。

【0240】

レシーバ251-1乃至251-Lは、レシーバ201と同様の構成を有する据え置き型の装置で、それぞれHDD252-1乃至252-Lに接続されている。レシーバ251はまた、レシーバ201と同様に、コンテンツを購入するための処理を実行することができるが、自分自身で課金を決済することができず、レシーバ51により代理決済されるようになされている。すなわち、例えば、この場合におけるレシーバ51の登録リスト（図47）およびレシーバ251-1の登録リスト（図48）に示すように、レシーバ251-i（=1, 2, ..., L）のSAMのIDに対応する「購入処理」には、“可”が設定され、“課金処理”

には、”不可”が設定され、そして「課金機器」には”SAM62のID”が、それぞれ設定されている。

【0241】

次に、レシーバ51が、レシーバ251において計上される課金を精算する場合の処理手順を、図49乃至図51のフローチャートを参照して説明する。

【0242】

ステップS361において、レシーバ51のSAM62は、カウンタ*i*に初期値1を設定し、ステップS362において、レシーバ51の相互認証モジュール71は、レシーバ251-*i* ($=1, 2, \dots, L$)の相互認証モジュール(図示せず)と相互認証する。この相互認証は、図35乃至図37を参照して説明した場合と同様であるので、その説明は省略する。

【0243】

ステップS363乃至S383においては、図43のステップS322乃至S342における場合と同様の処理が実行されるので、その説明は省略する。

【0244】

ステップS379において、レシーバ251-*i*が配送鍵*K_d*および登録リストを更新した後、またはレシーバ51が、「状態フラグ」に設定された動作制限情報に対応した処理を行った後、ステップS384に進み、レシーバ51のSAM62は、カウンタ*i*の値が、代理決済すべき機器の数(この例の場合、レシーバ251の数*L*)と等しいか否かを判定し、等しくないと判定した場合、ステップS385に進み、カウンタ*i*の値を1だけ増加させて、ステップS362に戻る。これにより、次のレシーバ251-*i*に対応して、それ以降の処理が実行される。

【0245】

ステップS384において、カウンタ*i*の値と、代理決済すべき機器の数*L*とが等しいと判定された場合、処理は終了される。

【0246】

ステップS363において、登録リストが改竄されていると判定された場合、またステップS364において、代理決済することができる機器ではないと判定

された場合、処理は、ステップ S 3 8 4 に進む。

【0247】

以上のようにして、L 個のレシーバ 2 5 1-1 乃至 2 5 1-L において、それぞれ計上される課金が、レシーバ 5 1 により代理決済される。なお、以上においては、レシーバ 5 1 が、一度に、レシーバ 2 5 1 の全てに対して、代理決済を行う場合を例として説明したが、図 4 3 乃至図 4 5 のフローチャートで説明したように、依頼があった機器に対してのみ代理決済を行うようにすることもできる。

【0248】

なお、以上において、図 4 3 のステップ S 3 2 3 および図 4 9 のステップ S 3 6 3 における、登録リストが改竄されているか否かの判定は、「登録リスト署名」に記憶されている署名を確認することで行われたが、入力されたデータを、6 4 ビットずつのブロックに切り分け、それを順次、処理時間の早いブロック暗号器に入力し、所定の検査用鍵で暗号化してそれを第 1 の出力とし、その第 1 び出力を遅延された第 2 の出力との排他的論理和により、データの改竄を確認する CBC (Cipher Block Chaining) モードを利用することもできる。

【0249】

図 5 2 は、ユーザホームネットワーク 5 の他の構成例を表している。なお、図中、図 1 のユーザホームネットワーク 5 における場合と対応する部分については、同一の符号を付してある。すなわち、レシーバ 2 0 1 および HDD 2 0 2 に代わり、レシーバ 3 0 1、レシーバ 4 0 1、および HDD 4 0 2 が設けられている。

【0250】

図 5 3 は、レシーバ 3 0 1 の機能的構成例を表している。レシーバ 3 0 1 は、レシーバ 2 0 1 の SAM 2 1 2 乃至通信部 2 1 5 と基本的に同様の機能を有する、SAM 3 1 1 乃至通信部 3 1 4 を有しているが、レシーバ 2 0 1 の、通信部 2 1 1、インタフェース 2 1 6、表示制御部 2 1 7、および入力制御部 2 1 8 に対応する機能を有しない、携帯型の機器である。

【0251】

レシーバ 3 0 1 は、HDD に接続されていないので、コンテンツは、図 5 4 に示すような形態を有する、外部記憶部 3 1 2 の利用情報記憶部 3 1 2 A に、コンテ

ンツ鍵K c o（保存鍵K s a v eで暗号化されている）およびUCSと対応して記憶される。

【0252】

図55に示すようなレシーバ301の登録リストは、記憶モジュール323に記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ301のSAM311のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が（「有効期限」の欄に）記憶され、登録リストのバージョン番号が（「バージョン番号」の欄に）記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ301には、レシーバ51の1機の機器が接続されているので、自分自身を含む合計値2が（「接続されている機器数」の欄に）記憶されている。リスト部には、図30のレシーバ51の登録リストの、レシーバ301の登録条件が記憶されているが、この場合、「登録条件署名」および「登録リスト署名」は、削除されている。これは、登録リストの署名の確認後、取り除かれたためで、これにより、記憶モジュール323の記憶容量を節約することができる。なお、この例の場合、1つの署名あたり、40バイトが必要とされる。

【0253】

レシーバ301は、サービスプロバイダ2およびEMDサービスセンタ1と通信を行うことができないので、コンテンツを購入する処理を行うことができない。そのため、「購入処理」には、“不可”が記憶されている。このように、レシーバ301においては、コンテンツの購入がなされないので、課金は計上されない。そのため「課金処理」には“不可”が、そして「課金機器」には、“なし”が記憶される。

【0254】

レシーバ301は、この例の場合、接続されるレシーバ51から、コンテンツの供給を受けるようになされているので、「コンテンツ供給機器」には、レシーバ51のSAM62のIDが記憶されている。

【0255】

「状態フラグ」には、この例の場合“なし”が設定されている。「登録条件署

名」および「登録リスト署名」には、所定の署名が記憶されている。

【0256】

図56は、レシーバ401の機能的構成例を表している。レシーバ401は、レシーバ201のSAM212乃至入力制御部218と基本的に同様の機能を有する、SAM311乃至入力制御部417を有しているが、レシーバ201の通信部211に対応する機能を有しない、据え置き型の機器である。

【0257】

HDD402には、コンテンツ等の他、図57に示すような、レシーバ401の登録リストが記憶されている。この登録リストの対象SAM情報部には、この登録リストを保有するレシーバ401のSAM411のIDが（「対象SAMID」の欄に）記憶され、その登録リストの有効期限が記憶され、登録リストのバージョン番号が記憶され、そして接続されている機器の数（自分自身を含む）、この例の場合、レシーバ401には、レシーバ51の1機の機器が接続されているので、自分自身を含む合計値2が（「接続されている機器数」の欄に）記憶されている。

【0258】

リスト部の「SAMID」には、レシーバ401のSAM411のIDが記憶され、「ユーザID」には、レシーバ401のユーザのIDが記憶される。レシーバ401は、サービスプロバイダ2およびEMDサービスセンタ1と通信を行うことができないので、コンテンツを購入する処理を行うことができない。そのため、「購入処理」には、“不可”が記憶されている。

【0259】

レシーバ401においては、コンテンツの購入がなされないので、課金は計上されない。そのため「課金処理」には“不可”が、「課金機器」には、“なし”が記憶される。レシーバ401は、接続されるレシーバ51からコンテンツの供給を受けるようになされているので、「コンテンツ供給機器」には、レシーバ51のSAM62のIDが記憶されている。

【0260】

「状態フラグ」には、この例の場合“なし”が設定されている。「登録条件署名」および「登録リスト署名」には、所定の署名が記憶されている。

【0261】

なお、この例の場合、レシーバ51の登録リストは、図58に示すように、レシーバ51の登録リストの他、図55の登録リストに示されるレシーバ301の登録条件、および図57の登録リストに示されるレシーバ401の登録条件が設定されている。

【0262】

次に、レシーバ51が、レシーバ301に代わり、コンテンツの購入処理を実行する場合の処理手順を、図59のフローチャートを参照して説明する。ステップS401において、レシーバ51は、レシーバ301と相互認証を行う。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ301のSAM311のIDを取得し、レシーバ301と一時鍵Ktempを共有する。

【0263】

ステップS402において、レシーバ51のSAM62は、HDD52に記憶されている登録リストが改竄されているか否かを判定する。具体的には、登録リストの「登録リスト署名」に記憶されている署名が、公開鍵暗号の公開鍵で復号され、それ結果（ハッシュ値）と、その登録リストのデータの全体のハッシュ値とが、等しいか否かが判定される。

【0264】

ステップS402で、登録リストが改竄されていないと判定された場合、ステップS403に進み、レシーバ51のSAM62は、代理購入の依頼があったレシーバ301が、代理購入することができる機器であるか否かを判定する。具体的には、ステップS401で取得されたSAM311のIDが、登録リストの「SAMID」に登録され、そしてそれに対応する「コンテンツ供給機器」にSAM62が登録されているか否かが判定される。この例の場合、レシーバ51の登録リスト（図58）の「SAMID」には、レシーバ301のSAM311のIDが設定され、そしてそれに対応する「コンテンツ供給機器」には、SAM62のIDが設定されているので、ステップS403において、レシーバ301が、代理購入することができる機器であると判定され、ステップS404に進む。

【0265】

ステップS404において、レシーバ51のSAM62は、代理購入が可能であることを示す所定の信号を、通信部65を介してレシーバ301に送信する。

【0266】

レシーバ301のSAM311は、レシーバ51から、代理購入が可能であることを示す信号を受信すると、ステップS405において、レシーバ301のデータ検査モジュール325は、購入するコンテンツAを記憶する、外部記憶部312の利用情報記憶部312AのブロックBPを検出する。

【0267】

次に、ステップS406において、レシーバ301のデータ検査モジュール325は、ステップS405で検出した、利用情報記憶部312AのブロックBPのデータの全体にハッシュ関数を適用してハッシュ値を算出し、記憶モジュール323に記憶されている、検出されたブロックBPに対応する検査値HPと一致しているか否かを判定する。それらの値が一致すると判定された場合、すなわち、利用情報記憶部312Aの、ステップS405で検出されたブロックBPのデータが改竄されていない場合、ステップS407に進み、SAM311は、コンテンツの供給を受け取ることが可能であることを示す所定の信号を、通信部314を介して、レシーバ51に送信する。

【0268】

ステップS408において、レシーバ51のSAM62（課金モジュール72）は、選択されたUCPの「利用内容」とPTに基づいて、UCSおよび課金情報を作成する。具体的には、レシーバ51の表示制御部67が、UCPA、B（図9）、およびPTA-1、A-2（図17）、B-1、B-2（図19）の内容を、図示せぬ表示部に出力し、ユーザに提示する。ユーザは、提示されたこれらの情報から、この例の場合、UCPAの「利用内容11」およびPTA-1を選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部68は、ユーザの操作に対応する信号（UCPAの「利用内容11」のIDとPTA-1のID）を操作部から受信し、それをSAM62に出力する。SAM62の課金モジュール72は、入力制御部68からのUCPAの「利用内容11」のIDとPTA-1のIDに基づいて、UCSAおよび

課金情報Aを作成する。

【0269】

なお、この例の場合、レシーバ301は、UCPやPTの内容を表示する表示部や、ユーザが、利用内容等を選択することができる操作部を有していない。そこで、このように、レシーバ301に接続され、表示部および操作部を有するレシーバ51を利用して、ユーザは、UCPの内容やPTを選択する。

【0270】

次に、ステップS409において、レシーバ51のSAM62は、ステップS408で作成した課金情報Aを記憶モジュール73に記憶させ、また作成したUCSAを、コンテンツ鍵KcoA、およびその署名とともに一時鍵Ktempで暗号化し、レシーバ301に送信する。なお、この処理が実行されるタイミングで、HDD52に記憶されているコンテンツAも一時鍵Ktempで暗号化され、レシーバ301に送信される。また、レシーバ51は、UCSAおよびコンテンツ鍵KcoAを、レシーバ301に送信した後、消去（破棄）する。これにより、コンテンツAを利用する権利は、レシーバ301のみにより保持されるようになる。

【0271】

次に、ステップS410において、レシーバ301のSAM311は、ステップS409でレシーバ51から送信されてきたUCSA、コンテンツ鍵KcoA、およびその署名、並びにコンテンツAを受信し、一時鍵Ktempで復号する。ステップS411において、レシーバ301の復号／暗号化モジュール324は、ステップS410で受信された署名を確認し、レシーバ51から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図37のステップS83における処理と同様であるので、その説明は省略する。

【0272】

ステップS411において、レシーバ51から送信されてきたデータが改竄されていないと判定した場合、ステップS412に進み、レシーバ301のSAM311は、ステップS410で受信されたUCSA、コンテンツ鍵KcoA、およびコンテンツAを外部記憶部312の利用情報記憶部312Aの、ステップS405で検出されたブロックBPに記憶させる。

【0273】

次に、ステップS413において、レシーバ301のデータ検査モジュール325は、ステップS412で、UCSA、コンテンツ鍵KcoA、およびコンテンツAが記憶された外部記憶部312の利用情報記憶部312AのブロックBPのデータにハッシュ関数を適用して、ハッシュ値を算出する。そして、ステップS414において、データ検査モジュール325は、算出したハッシュ値を、記憶モジュール323に記憶されている、ブロックBPに対応する検査値HPに上書きする。

【0274】

ステップS402において、登録リストが改竄されていると判定された場合、ステップS403において、レシーバ301が代理決済すべき機器でないと判定された場合、およびステップS406において、検出されたブロックBPが改竄されていると判定された場合、処理は終了される。

【0275】

ステップS411において、レシーバ51からのデータが改竄されていると判定された場合、ステップS415に進み、レシーバ301のSAM311は、その旨をレシーバ51に通知する等の処理を実行する。その後、ステップS409に戻る。すなわち、これにより、UCSA、コンテンツ鍵KcoA、およびその署名、並びにコンテンツAが、再度、レシーバ301に送信される。なお、この例の場合、レシーバ51からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより処理が終了された場合、ステップS409で、レシーバ51の記憶モジュール73に記憶された課金情報Aを削除するようにすることもできるが、課金情報Aに代理購入処理が成功しなかった（失敗した）回数を設定するようにして、その代理購入処理の失敗回数が所定の回数を超えた場合、登録リストの、レシーバ301のSAM311のIDに対応する「状態フラグ」に”制限あり”とし、レシーバ301において行われる処理を制限するようにすることもできる。

【0276】

以上のようにして、レシーバ51により、レシーバ301に対する、コンテン

ツの代理購入が行われるが、課金情報は、レシーバ301に供給されずに、レシーバ51に保持されているので、ここで計上された課金は、レシーバ51自身の課金として精算される（図42のフローチャートにより決済される）。

【0277】

次に、レシーバ301が複数のコンテンツを購入する場合の、レシーバ51による代理購入処理の処理手順を、図60のフローチャートを参照して説明する。ステップS431において、レシーバ301と相互認証を行う。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ301のSAM311のIDを取得し、レシーバ301と一時鍵Ktempを共有する。

【0278】

ステップS432乃至S434においては、図59のステップS402乃至S404における場合と同様の処理が実行されるので、その説明は省略する。

【0279】

ステップS435において、レシーバ301のSAM311は、カウンタjの値を初期値1に設定し、次に、レシーバ301のデータ検査モジュール325は、コンテンツj（=1, 2, 3・・・K）を記憶する、外部記憶部312の利用情報記憶部311AのブロックBPを検出する。

【0280】

ステップS437乃至S446においては、図59のステップS406乃至S415における場合と同様の処理が実行されるので、その説明は省略する。

【0281】

ステップS447において、レシーバ301のSAM311は、カウンタjの値が、購入したいコンテンツの数Kと一致するか否かを判定し、一致しない場合、ステップS448に進み、カウンタjの値を1だけ増加させ、ステップS436に戻る。これにより、次の、代理購入されるコンテンツjに対応する処理が実行される。

【0282】

ステップS447で、カウンタjの値が、代理するコンテンツの数Kと等しい

と判定された場合、処理は終了される。

【0283】

以上のようにして、複数のコンテンツが代理購入される。

【0284】

次に、レシーバ301が、複数のコンテンツを購入する場合の、レシーバ51による代理購入処理の他の手順を、図61のフローチャートを参照して説明する。この例の場合も、図60における場合と同様に、レシーバ301が、K個のコンテンツを購入するものとする。

【0285】

ステップS461において、レシーバ51は、レシーバ301と相互認証を行う。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ301のSAM311のIDを取得し、レシーバ301と一時鍵Ktempを共有する。

【0286】

ステップS462、S463においては、図59のステップS402、S403における場合と同様の処理が実行されるので、その説明は省略する。

【0287】

ステップS463において、レシーバ301が、代理購入することができる機器であると判定した場合、レシーバ51のSAM62は、コンテンツを記憶することができる記憶容量の通知を要求する所定の信号を、レシーバ301に送信する。

【0288】

レシーバ51から送信された、記憶容量の通知を要求する信号を受信すると、ステップS465において、レシーバ301のSAM311は、コンテンツを記憶することができる、いわゆる、空いている、外部記憶部312の利用情報記憶部312A（ブロックBP）の記憶容量を調査し、それをレシーバ51に通知する。

【0289】

ステップS466において、レシーバ51は、ステップS465で通知された記憶容量に記憶することができる k ($=\leq K$) 個のコンテンツのIDを、レシーバ301に通知する。例えば、通知されたレシーバ301の外部記憶部312の空いている容量が、十分大きい場合、購入したい K 個のコンテンツの全てのIDが通知され、またその容量が十分大きくない場合、その容量に記憶することができる分だけのコンテンツのIDが通知される。

【0290】

ステップS467において、レシーバ301のデータ検査モジュール325は、ステップS466でIDが通信された k 個のコンテンツを記憶する、外部記憶部312の利用情報記憶部312Aの k 個のブロックBPを検出する。ステップS468において、レシーバ301のデータ検査モジュール325は、ステップS467で検出した利用情報記憶部312Aの k 個のブロックBPのそれぞれのデータにハッシュ関数を適用してハッシュ値を算出し、記憶モジュール323に記憶されている、検出された k 個のブロックBPに対応する検査値HPと一致しているか否かをそれぞれ判定し、 k 個のブロックBPのデータが改竄されているか否かを判定する。

【0291】

ステップS468において、ステップS467で検出された全てのブロックBPのデータが改竄されていないと判定された場合、ステップS469に進み、レシーバ301のSAM311は、ステップS466でIDが通知された k 個のコンテンツを受け取ることが可能であることを示す信号を、通信部314を介して、レシーバ51に送信する。

【0292】

ステップS470において、レシーバ51のSAM62（課金モジュール72）は、 k 個のコンテンツに対応する k 個のUCSおよび k 個の課金情報を作成する。なお、ここでの具体的な処理は、図59のステップS408における場合と、基本的に同様であるので、その説明は省略する。

【0293】

次に、ステップS471において、レシーバ51のSAM62は、作成した k 個

の課金情報を記憶モジュール 73 に記憶させ、また作成した k 個の UCS を、k 個のコンテンツ鍵 K_{co} 、およびその署名とともに一時鍵 K_{temp} で暗号化し、レシーバ 301 に送信する。なお、この処理が実行されるタイミングで、HDD 52 に記憶されている k 個のコンテンツ（購入される）も一時鍵 K_{temp} で暗号化され、レシーバ 301 に送信される。

【0294】

次に、ステップ S472 において、レシーバ 301 の SAM 311 は、ステップ S471 でレシーバ 51 から送信されてきた k 個の UCS、k 個のコンテンツ鍵 K_{co} 、および署名、並びに k 個のコンテンツをデータを受信し、一時鍵 K_{temp} で復号する。ステップ S473 において、レシーバ 301 の復号／暗号化モジュール 324 は、ステップ S472 で受信された署名を確認し、レシーバ 51 から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図 37 のステップ S83 における処理と同様であるので、その説明は省略する。

【0295】

ステップ S473 において、レシーバ 51 から送信されてきたデータが改竄されていないと判定された場合、ステップ S474 に進み、レシーバ 301 の SAM 311 は、ステップ S472 で受信された k 個の UCS、k 個のコンテンツ鍵 K_{co} 、および k 個のコンテンツを外部記憶部 312 の利用情報記憶部 312A の、ステップ S467 で検出された k 個のブロック BP に記憶させる。

【0296】

ステップ S475 において、レシーバ 301 のデータ検査モジュール 325 は、ステップ S474 で、UCS、コンテンツ鍵 K_{co} 、およびコンテンツが記憶された外部記憶部 312 の利用情報記憶部 312A の k 個のブロック BP のデータにハッシュ関数を適用して、それぞれのハッシュ値を算出し、それを、ステップ S476 において、記憶モジュール 323 に記憶されている、対応する検査値 H_P に上書きする。その後、処理は終了される。

【0297】

ステップ S462 において、登録リストが改竄されていると判定された場合、

ステップS463において、レシーバ301が代理決済すべき機器でないと判定された場合、およびステップS468において、検出されたブロックBPが改竄されていると判定された場合、処理は終了される。

【0298】

ステップS473において、レシーバ51からのデータが改竄されていると判定された場合、ステップS477に進み、レシーバ301のSAM311は、その旨をレシーバ51に通知する等の処理を実行する。その後、ステップS471に戻る。すなわち、これにより、k個のUCS、k個のコンテンツ鍵Kco、およびその署名、並びにk個のコンテンツが、再度、レシーバ301に送信される。なお、この場合も、レシーバ51からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより処理が終了された場合、ステップS471で、レシーバ51の記憶モジュール73に記憶されたk個の課金情報を削除するようにすることもできるが、k個の課金情報のそれぞれに代理購入処理の失敗回数を設定するようにして、その回数が所定の回数を越えた場合、登録リストの、レシーバ301のSAM311のIDに対応する「状態フラグ」に”制限あり”とし、レシーバ301において行われる処理を制限することもできる。

【0299】

次に、レシーバ51が、レシーバ401に代わり、コンテンツを購入する場合（代理購入する場合）の処理手順を、図62、図63のフローチャートを参照して説明する。レシーバ51は、レシーバ401から、購入したいコンテンツのIDと、所定の代理購入を依頼する所定の信号を受信すると、ステップS501において、レシーバ51は、レシーバ401と相互認証を行う。この相互認証は、図37を参照して説明した場合と同様であるので、その説明は省略するが、これにより、レシーバ51の相互認証モジュール71は、レシーバ401のSAM411のIDを取得し、レシーバ401と一時鍵Ktempを共有する。

【0300】

ステップS502において、レシーバ51のSAM62は、HDD52に記憶されている登録リストが改竄されているか否かを判定し、登録リストが改竄されてい

いと判定された場合、ステップ S 5 0 3 に進み、代理購入の依頼のあったレシーバ 4 0 1 が、代理購入すべき機器であるか否かを判定する。ここでの具体的な処理は、図 5 9 のステップ S 4 0 3 における場合と同様であるので、その説明は省略する。ステップ S 5 0 3 で、レシーバ 4 0 1 が、代理決済すべき機器であると判定した場合、レシーバ 5 1 の SAM 6 2 は、ステップ S 5 0 4 に進み、予め通知された、レシーバ 5 0 1 が購入したいコンテンツの UCP および PT を、署名を付して、レシーバ 4 0 1 に送信する。なお、UCP、PT、およびコンテンツは、サービスプロバイダセキュアコンテナに含まれているので、そのまま渡してもよい。

【 0 3 0 1 】

ステップ S 5 0 5 において、レシーバ 4 0 1 の SAM 4 1 1 は、レシーバ 5 1 から送信された UCP、PT、およびその署名を受信し、ステップ S 5 0 6 において、署名を確認し、レシーバ 5 1 から送信されてきたデータが改竄されているか否かを判定する。この署名の確認は、図 3 7 のステップ S 8 3 における処理と同様であるので、その説明は省略する。

【 0 3 0 2 】

ステップ S 5 0 6 において、レシーバ 5 1 から送信されてきたデータが改竄されていないと判定した場合、レシーバ 4 0 1 の SAM 4 1 1 は、ステップ S 5 0 7 に進み、購入するコンテンツに対応するコンテンツ鍵 K c o を記憶する、外部記憶部 4 1 2 の利用情報記憶部 4 1 2 A のブロック BP (図示せず) を検出する。

【 0 3 0 3 】

次に、ステップ S 5 0 8 において、レシーバ 4 0 1 のデータ検査モジュール 4 2 5 は、ステップ S 5 0 7 で検出された利用情報記憶部 4 1 2 A のブロック BP に記憶されているデータの全体にハッシュ関数を適用してハッシュ値を算出し、記憶モジュール 4 2 3 に記憶されている、検出されたブロック BP に対応する検査値 HP と一致するか否かを判定する。それらの値が一致すると判定された場合、すなわち、利用情報記憶部 4 1 2 A の、検出されたブロック BP が改竄されていない場合、ステップ S 5 0 9 に進む。

【 0 3 0 4 】

ステップ S 5 0 9 において、レシーバ 4 0 1 の SAM 4 1 1 は、ステップ S 5 0

5で受信されたUCPの「利用内容」とPTのIDをレシーバ51の通知する。なお、実際は、この処理に先だって、レシーバ401の表示制御部416が、ステップS505で受信されたUCPおよびPTの内容を、図示せぬ表示部に出力し、ユーザに提示する。ユーザは、提示されたこれらの情報から、UCPの利用内容およびPTを選択する操作を、図示せぬ操作部に対して行う。これにより、入力制御部417は、ユーザの操作に対応する信号（UCPの「利用内容」のIDとPTのID）を操作部から受信し、それをSAM411に出力する。SAM411は、入力制御部417からの情報を、通信部414に介してレシーバ51に送信する。

【0305】

このように、ユーザが、UCPの内容およびPTを選択することができる機能をするレシーバ401に対しては、UCPおよびPT（購入するコンテンツのIDおよび選択項目）が、レシーバ51から送信される。なお、UCPおよびPTに代えて、

ステップS510において、レシーバ51のSAM62は、レシーバ401から通知されたUCPの「利用内容」のIDおよびPTのID（購入するコンテンツのIDおよび選択項目）に基づいて、課金情報およびUCSを作成する。次に、ステップS511において、レシーバ51のSAM62は、ステップS510で作成した課金情報を記憶モジュール73に記憶させ、そして作成したUCSを、購入されるコンテンツに対応するコンテンツ鍵Kco、およびそれらの署名とともにレシーバ401に送信する。なお、この処理が実行されるタイミングで、HDD52に記憶されている、購入されるコンテンツもレシーバ401に送信される。なお、サービスプロバイダセキュアコンテナをレシーバ401に送信し、レシーバ401が、改竄チェック、利用内容の選択、および要求を出して、レシーバ51で購入し、UCSや鍵を渡すようにすることもできる。

【0306】

次に、ステップS512において、レシーバ401のSAM411は、ステップS511でレシーバ51から送信されてきたUCS、コンテンツ鍵Kco、およびその署名、並びにコンテンツを受信し、一時鍵Ktempで復号する。ステップS513において、レシーバ401の復号／暗号化モジュール424は、ステップS512で受信された署名を確認し、レシーバ51から送信されてきたデータ

が改竄されているか否かを判定する。この署名の確認は、図 37 のステップ S 83 における処理と同様であるので、その説明は省略する。

【0307】

ステップ S 513 において、レシーバ 51 から送信されてきたデータが改竄されていないと判定された場合、ステップ S 514 に進み、レシーバ 401 の SAM 411 は、ステップ S 505 で受信された UCP、PT、およびコンテンツを HDD 402 に記憶させる。次に、ステップ S 515 において、SAM 411 は、ステップ S 512 で受信された UCS とコンテンツ鍵 K_{co} を、外部記憶部 412 の利用情報記憶部 412A の、ステップ S 507 で検出されたブロック BP に記憶させる。

【0308】

次に、ステップ S 516 において、レシーバ 401 のデータ検査モジュール 425 は、ステップ S 515 で、UCS とコンテンツ鍵 K_{co} が記憶された外部記憶部 412 の利用情報記憶部 412A のブロック BP のデータにハッシュ関数を適用して、ハッシュ値を算出し、それを、ステップ S 517 において、記憶モジュール 423 に記憶されている、対応する検査値 HP に上書きする。

【0309】

ステップ S 502 において、登録リストが改竄されていると判定された場合、ステップ S 503 において、レシーバ 401 が代理決済すべき機器でないと判定された場合、およびステップ S 508 において、利用情報が記憶されるブロック BP が改竄されていると判定された場合、処理は終了される。

【0310】

ステップ S 506 において、レシーバ 51 からのデータが改竄されていると判定された場合、ステップ S 518 に進み、レシーバ 401 の SAM 411 は、その旨をレシーバ 51 に通知する等の処理を実行する。その後、ステップ S 504 に戻る。すなわち、これにより、UCP、PT、およびその署名が、再度、レシーバ 401 に送信される。なお、この例の場合、レシーバ 51 からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。

【0311】

ステップ S 5 1 3 において、レシーバ 5 1 からのデータが改竄されていると判定された場合、ステップ S 5 1 9 に進み、レシーバ 4 0 1 の SAM 4 1 1 は、その旨をレシーバ 5 1 に通知する等の処理を実行する。その後、ステップ S 5 1 1 に戻る。すなわち、これにより、UCS、コンテンツ鍵 K c o、およびその署名、並びにコンテンツが、再度、レシーバ 4 0 1 に送信される。なお、この例の場合、レシーバ 5 1 からの、この送信は、予め決められた回数だけ行われるものとし、その回数を越えた場合、処理は終了されるものとする。また、これにより終了された場合、ステップ S 5 1 0 で、レシーバ 5 1 の記憶モジュール 7 3 に記憶された課金情報を削除するようにすることもできるが、課金情報に代理購入処理の失敗回数を設定するようにして、その回数が所定の回数を越えたとき、登録リストのレシーバ 4 0 1 の SAM 4 1 1 の ID に対応する「状態フラグ」に”制限あり”とし、レシーバ 4 0 1 における処理を制限するようにすることもできる。

【0312】

なお、コンテンツは、音楽データを例に説明したが、音楽データに限らず、動画像データ、静止画像データ、文書データ、またはプログラムデータでもよい。その際、圧縮は、コンテンツの種類に適した方式、例えば、画像であれば MPEG (Moving Picture Experts Group) などが利用される。ウォーターマークも、コンテンツの種類に適した形式のウォーターマークが利用される。

【0313】

また、共通鍵暗号は、ブロック暗号である DES を使用して説明したが、NTT (商標) が提案する FEAL、IDEA (International Data Encryption Algorithm)、または 1 ビット乃至数ビット単位で暗号化するストリーム暗号などでもよい。

【0314】

さらに、コンテンツおよびコンテンツ鍵 K c o の暗号化は、共通鍵暗号方式を利用するとして説明したが、公開鍵暗号方式でもよい。

【0315】

なお、本明細書において、システムとは、複数の装置により構成される装置全体を表すものとする。

【0316】

また、上記したような処理を行うコンピュータプログラムをユーザに提供する提供媒体としては、磁気ディスク、CD-ROM、固体メモリなどの記録媒体の他、ネットワーク、衛星などの通信媒体を利用することができる。

【0317】

【発明の効果】

請求項1に記載の情報処理装置、請求項2に記載の情報処理方法、および請求項3に記載の提供媒体によれば、他の情報処理装置から、課金情報を受信し、管理装置に送信するようにしたので、課金情報に基づいて行われた決済処理に基づいて作成された動作制限情報に基づいて、動作を制御することができる。

【0318】

請求項4に記載の情報処理装置、請求項6に記載の情報処理方法、および請求項7に記載の提供媒体によれば、代理購入情報に対応して、使用許諾条件情報を作成し、暗号化された情報を復号するために必要な鍵とともに、他の情報処理装置に送信するようにしたので、他の情報処理装置が、暗号化された情報を復号して利用することができる。

【図面の簡単な説明】

【図1】

EMDシステムを説明する図である。

【図2】

EMDシステムにおける、主な情報の流れを説明する図である。

【図3】

EMDサービスセンタ1の機能的構成を示すブロック図である。

【図4】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する図である。

【図5】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の図である。

【図6】

EMDサービスセンタ1の配送用鍵Kdの送信を説明する他の図である。

【図7】

EMDサービスセンタ 1 の配送用鍵 K d の送信を説明する他の図である。

【図 8】

コンテンツプロバイダ 2 の機能的構成例を示すブロック図である。

【図 9】

UCPを説明する図である。

【図 1 0】

コンテンツの管理移動を説明する図である。

【図 1 1】

第 1 世代複製を説明する図である。

【図 1 2】

サービスコードおよびコンディションコードのコード値の例を示す図である。

【図 1 3】

UCPの利用条件として設定されたコード値の例を示す図である。

【図 1 4】

コンテンツプロバイダセキュアコンテナの例を示す図である。

【図 1 5】

コンテンツプロバイダ 2 の証明書の例を示す図である。

【図 1 6】

サービスプロバイダ 3 の機能の構成を示すブロック図である。

【図 1 7】

PTの例を示す図である。

【図 1 8】

PTの価格条件として設定されたコード値の例を示す図である。

【図 1 9】

他のPTの例を示す図である。

【図 2 0】

他のPTの価格条件として設定されたコード値の例を示す図である。

【図 2 1】

サービスプロバイダセキュアコンテナの例を示す図である。

【図 2 2】

サービスプロバイダ 3 の証明書の例を示す図である。

【図 2 3】

ユーザホームネットワーク 5 のレシーバ 5 1 の機能的構成例を示すブロック図である。

【図 2 4】

レシーバ 5 1 の SAM 6 2 の証明書の例を示す図である。

【図 2 5】

UCS の例を示す図である。

【図 2 6】

レシーバ 5 1 の外部記憶部 6 3 の利用情報記憶部 6 3 A の内部を説明する図である。

【図 2 7】

課金情報の例を示す図である。

【図 2 8】

レシーバ 5 1 の記憶モジュール 7 3 に記憶されている情報を示す図である。

【図 2 9】

基準情報 5 1 を説明する図である。

【図 3 0】

レシーバ 5 1 の登録リストの例を示す図である。

【図 3 1】

ユーザホームネットワーク 5 のレシーバ 2 0 1 の機能的構成例を示すブロック図である。

【図 3 2】

レシーバ 2 0 1 の登録リストの例を示す図である。

【図 3 3】

コンテンツの利用処理を説明するフローチャートである。

【図 3 4】

EMD サービスセンタ 1 がコンテンツプロバイダ 2 へ配送用鍵 K d を送信する処

理を説明するフローチャートである。

【図 3 5】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の動作を説明するフローチャートである。

【図 3 6】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 3 7】

コンテンツプロバイダ 2 と EMD サービスセンタ 1 との相互認証の他の動作を説明するフローチャートである。

【図 3 8】

コンテンツプロバイダ 2 がサービスプロバイダ 3 にコンテンツプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 3 9】

サービスプロバイダ 3 がレシーバ 5 1 にサービスプロバイダセキュアコンテナを送信する処理を説明するフローチャートである。

【図 4 0】

レシーバ 5 1 がサービスプロバイダセキュアコンテナを受信する処理を説明するフローチャートである。

【図 4 1】

レシーバ 5 1 がコンテンツを再生する処理を説明するフローチャートである。

【図 4 2】

課金を決済する処理を説明するフローチャートである。

【図 4 3】

代理決済処理の手順を説明するフローチャートである。

【図 4 4】

代理決済処理の手順を説明するフローチャートである。

【図 4 5】

代理決済処理の手順を説明するフローチャートである。

【図 4 6】

ユーザホームネットワーク 5 の他の構成例を示す図である。

【図 4 7】

ユーザホームネットワーク 5 のレシーバ 5 1 の登録リストの例を示す図である。

【図 4 8】

ユーザホームネットワーク 5 のレシーバ 2 5 1 の登録リストの例を示す図である。

【図 4 9】

代理決済処理の他の手順を説明するフローチャートである。

【図 5 0】

代理決済処理の他の手順を説明するフローチャートである。

【図 5 1】

代理決済処理の他の手順を説明するフローチャートである。

【図 5 2】

ユーザホームネットワーク 5 の他の構成例を示す図である。

【図 5 3】

レシーバ 3 0 1 の構成例を示す図である。

【図 5 4】

レシーバ 3 0 1 の利用情報記憶部 3 1 2 A の形態を示す図である。

【図 5 5】

レシーバ 3 0 1 の登録リストの例を示す図である。

【図 5 6】

レシーバ 4 0 1 の構成例を示す図である。

【図 5 7】

レシーバ 4 0 1 の登録リストの例を示す図である。

【図 5 8】

レシーバ 5 1 の登録リストの例を示す図である。

【図 5 9】

代理購入処理の手順を説明するフローチャートである。

【図60】

代理購入処理の他の手順を説明するフローチャートである。

【図61】

代理購入処理の他の手順を説明するフローチャートである。

【図62】

代理購入処理の他の手順を説明するフローチャートである。

【図63】

代理購入処理の他の手順を説明するフローチャートである。

【符号の説明】

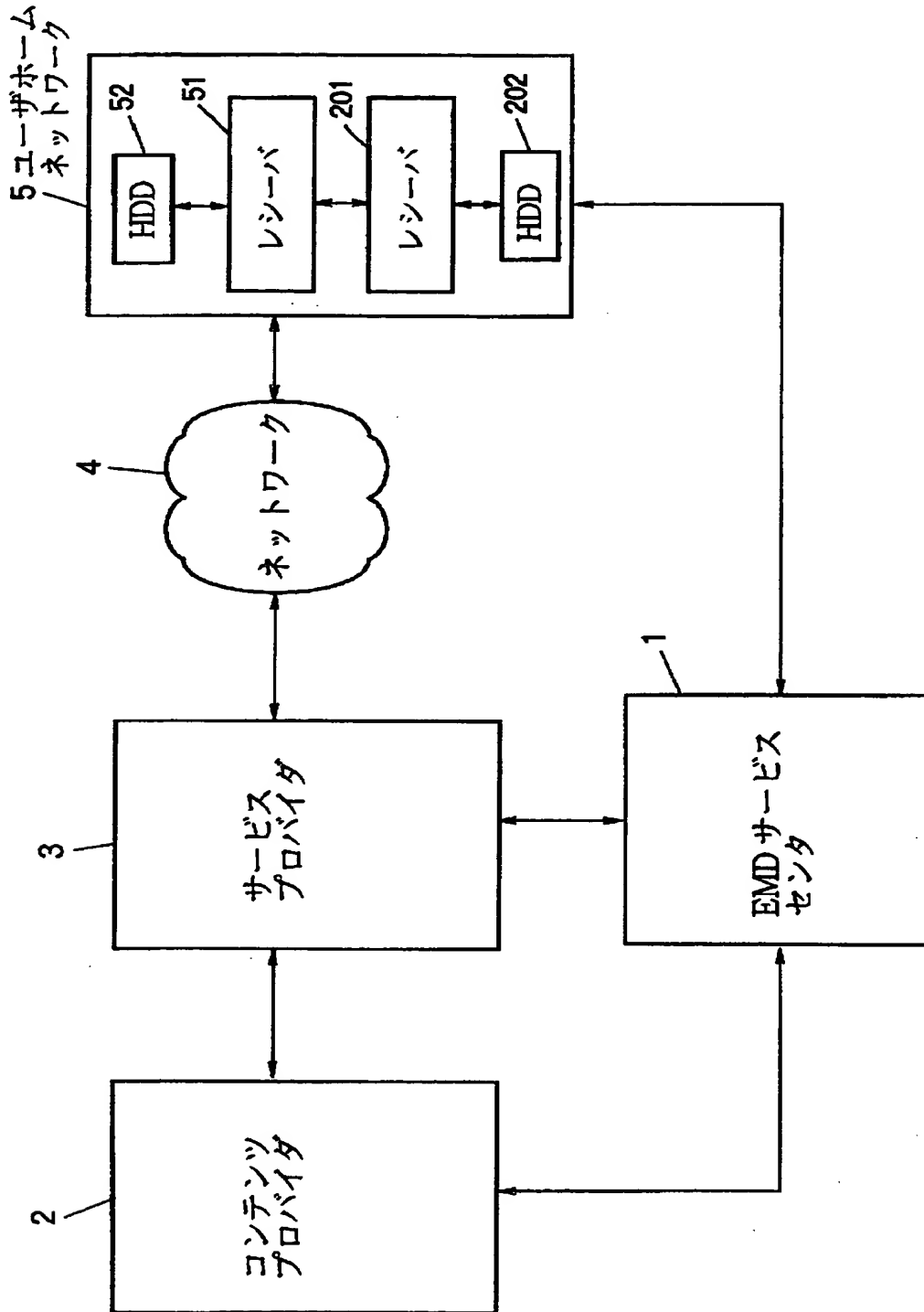
1 EMDサービスセンタ, 2 コンテンツプロバイダ, 3 サービスプロバイダ, 5 ユーザホームネットワーク, 11 サービスプロバイダ管理部, 12 コンテンツプロバイダ管理部, 13 著作権管理部, 14 鍵サーバ, 15 経歴データ管理部, 16 利益分配部, 17 相互認証部, 18 ユーザ管理部, 19 課金請求部, 20 出納部, 21 監査部, 31 コンテンツサーバ, 32 ウォータマーク付加部, 33 圧縮部, 34 暗号化部, 35 乱数発生部, 36 暗号化部, 37 ポリシー記憶部, 38 セキュアコンテナ作成部, 39 相互認証部, 41 コンテンツサーバ, 42 値付け部, 43 ポリシー記憶部, 44 セキュアコンテナ作成部, 45 相互認証部, 51 レシーバ, 52 HDD, 61 通信部, 62 SAM, 63 外部記憶部, 64 伸張部, 65 通信部, 66 インタフェース, 67 表示制御部, 68 入力制御部, 71 相互認証モジュール, 72 課金処理モジュール, 73 記憶モジュール, 74 復号/暗号化モジュール, 75 データ検査モジュール, 91 復号ユニット, 92 乱数発生ユニット, 93 暗号化ユニット, 101 相互認証モジュール, 102 復号モジュール, 103 復号モジュール, 104 伸張モジュール, 105 ウォータマーク付加モジュール, 201 レシーバ, 202 HDD, 211 通信部, 212 SAM, 213 外部記憶部, 214 伸張部, 215 通信部, 216 インタ

フェース, 217 表示制御部, 218 入力制御部, 221 相互認証
 モジュール, 222 課金処理モジュール, 223 記憶モジュール, 2
 24 復号/暗号化モジュール, 225 データ検査モジュール, 231
 復号ユニット, 232 乱数発生ユニット, 233 暗号化ユニット, 2
 41 相互認証モジュール, 242 復号モジュール, 243 復号モジュ
 ール, 244 伸張モジュール, 245 ウォータマーク付加モジュール,
 301 レシーバ, 311 SAM, 312 外部記憶部, 313 伸張
 部, 314 通信部, 321 相互認証モジュール, 322 課金処理モ
 ジュール, 323 記憶モジュール, 324 復号/暗号化モジュール,
 325 データ検査モジュール, 331 復号ユニット, 332 乱数発生
 ユニット, 333 暗号化ユニット, 341 相互認証モジュール, 34
 2 復号モジュール, 343 復号モジュール, 344 伸張モジュール,
 345 ウォータマーク付加モジュール, 401 レシーバ, 402 HD
 D, 411 SAM, 412 外部記憶部, 413 伸張部, 414 通信
 部, 415 インタフェース, 416 表示制御部, 417 入力制御部
 , 421 相互認証モジュール, 422 課金処理モジュール, 423
 記憶モジュール, 424 復号/暗号化モジュール, 425 データ検査モ
 ジュール, 431 復号ユニット, 432 乱数発生ユニット, 433
 暗号化ユニット, 441 相互認証モジュール, 442 復号モジュール,
 443 復号モジュール, 444 伸張モジュール, 445 ウォータマ
 ーク付加モジュール

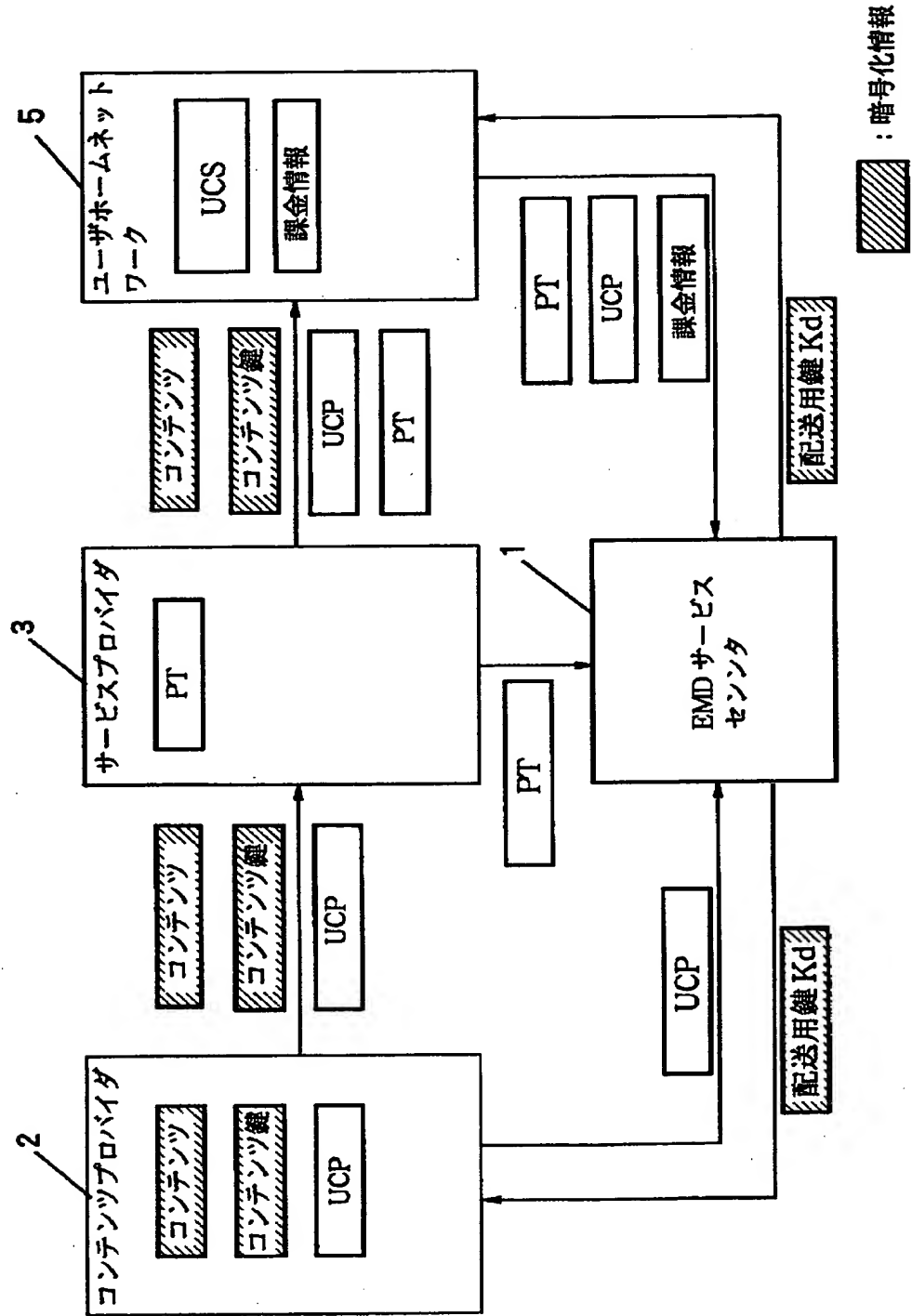
【書類名】

図面

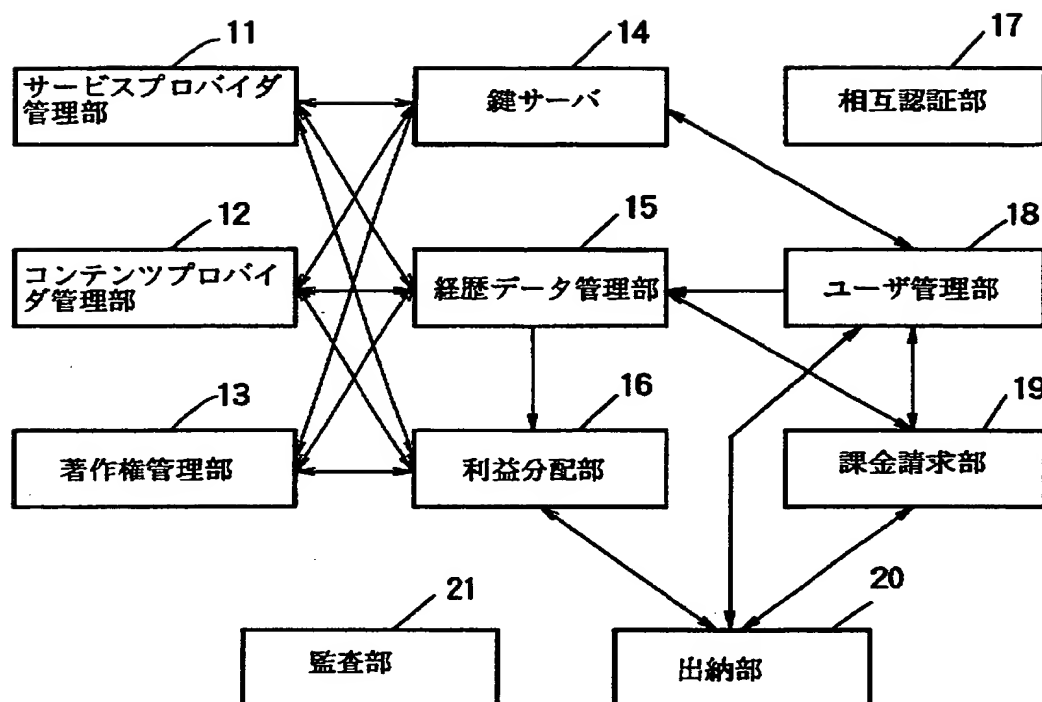
【図 1】



【図 2】

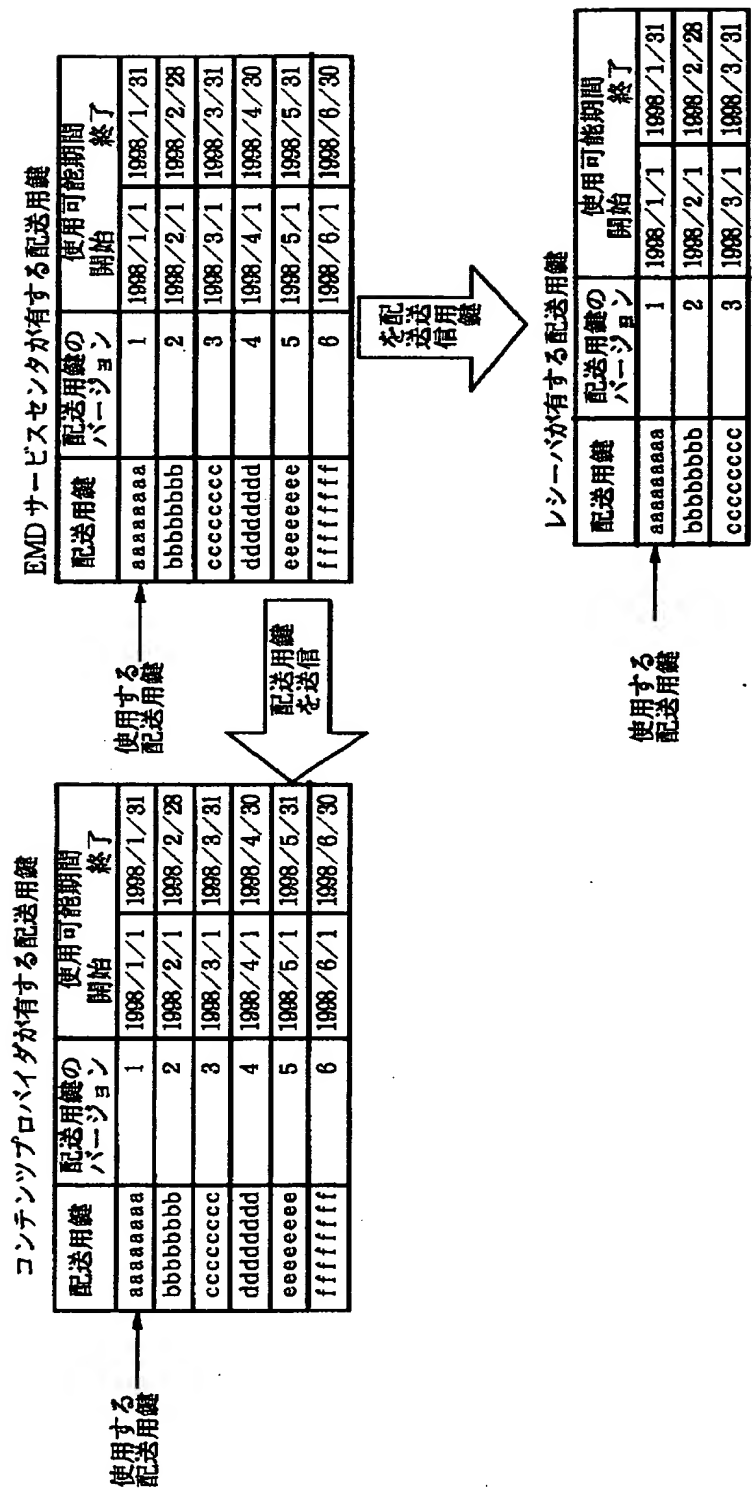


【図3】

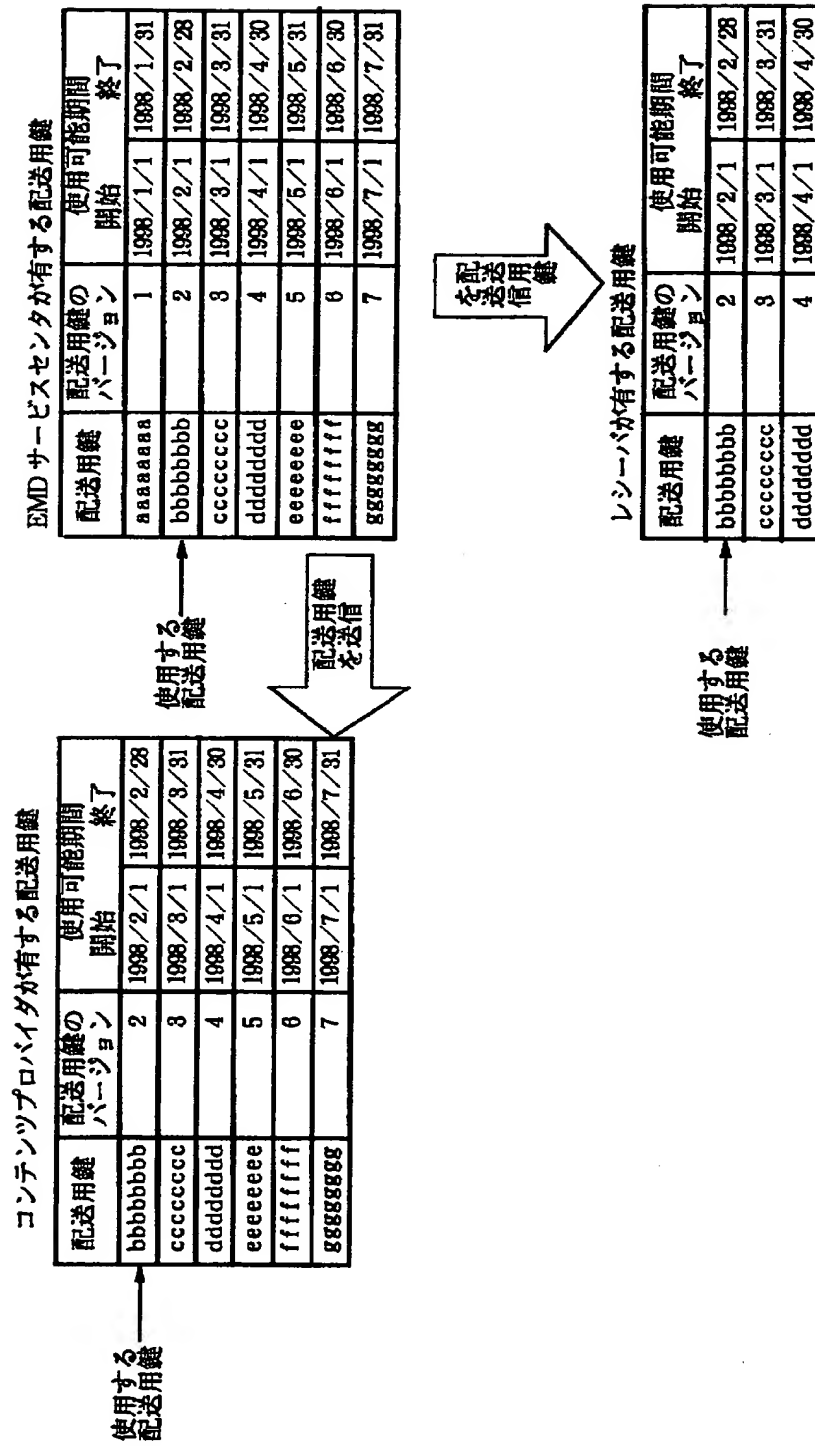


EMD サービスセンタ 1

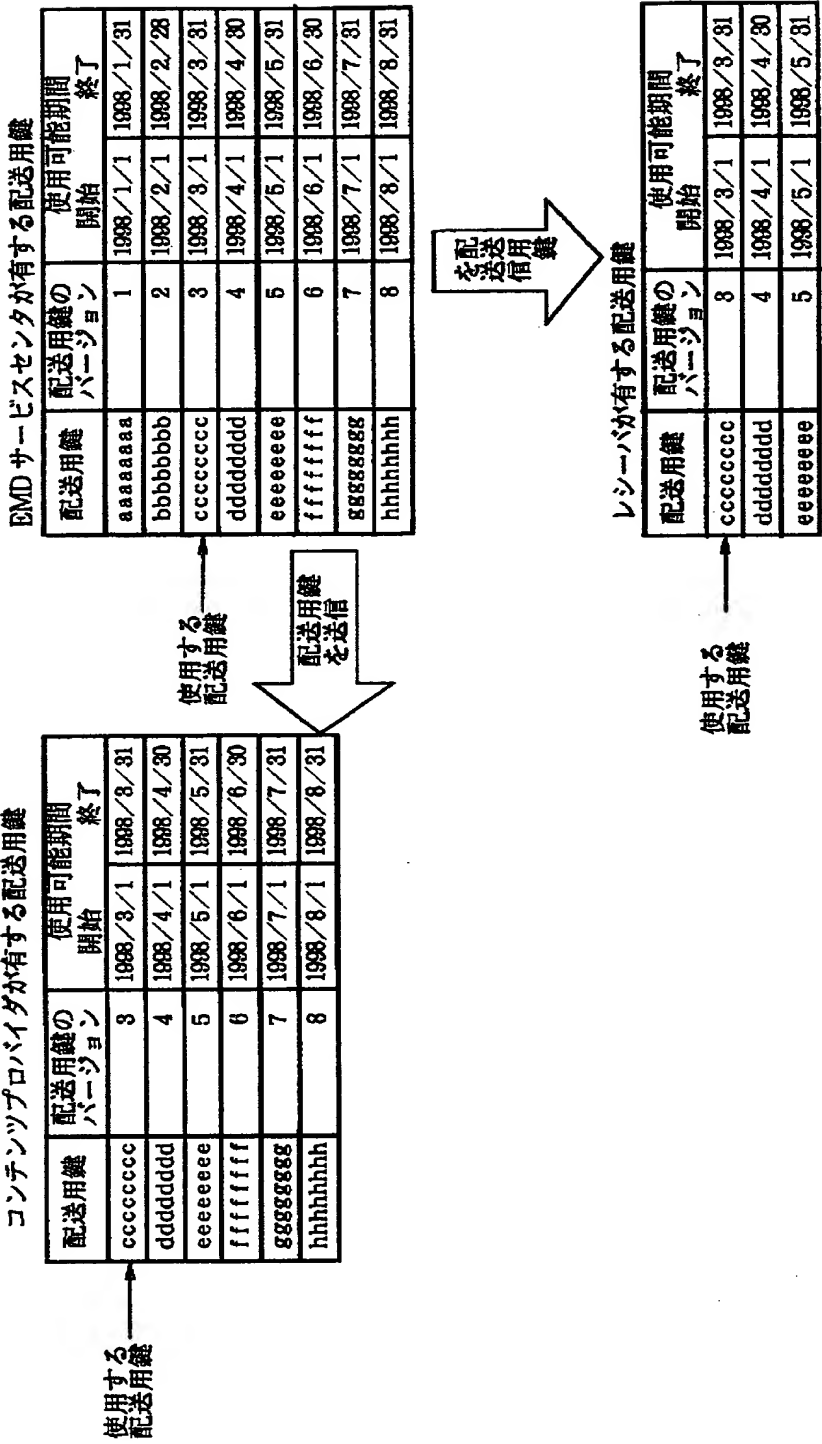
【 図 4 】



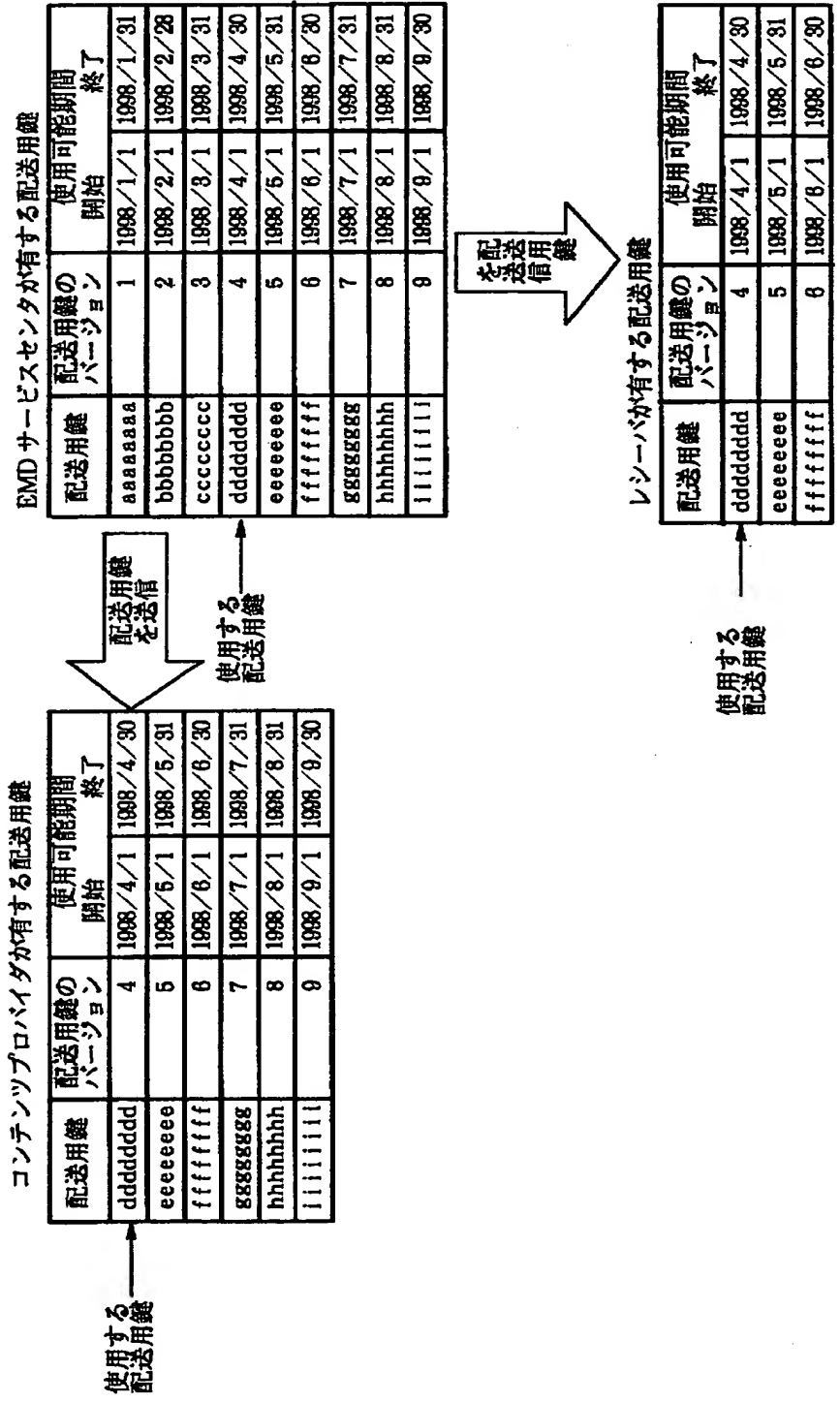
【図 5】



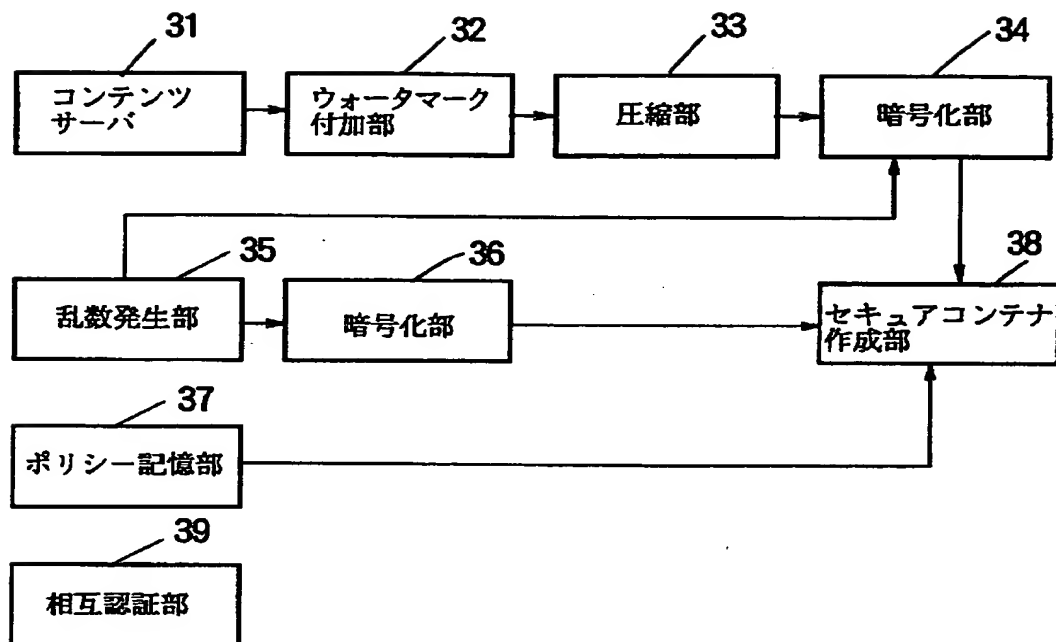
【図 6】



【図 7】



【図 8】



コンテンツプロバイダ 2

【図 9】

(B)

コンテンツの ID	コンテンツ A の ID
コンテンツプロバイダの ID	コンテンツプロバイダ 2 の ID
UCP の ID	ucpB の ID
UCP の有効期限	ucpB の有効期限
利用条件 20	ユーザ条件 20
	機器条件 20
利用内容 21	ID 21
	形式 21
	パラメータ 21
	管理移動許可情報 21
利用内容 22	ID 22
	形式 22
	パラメータ 22
	管理移動許可情報 22

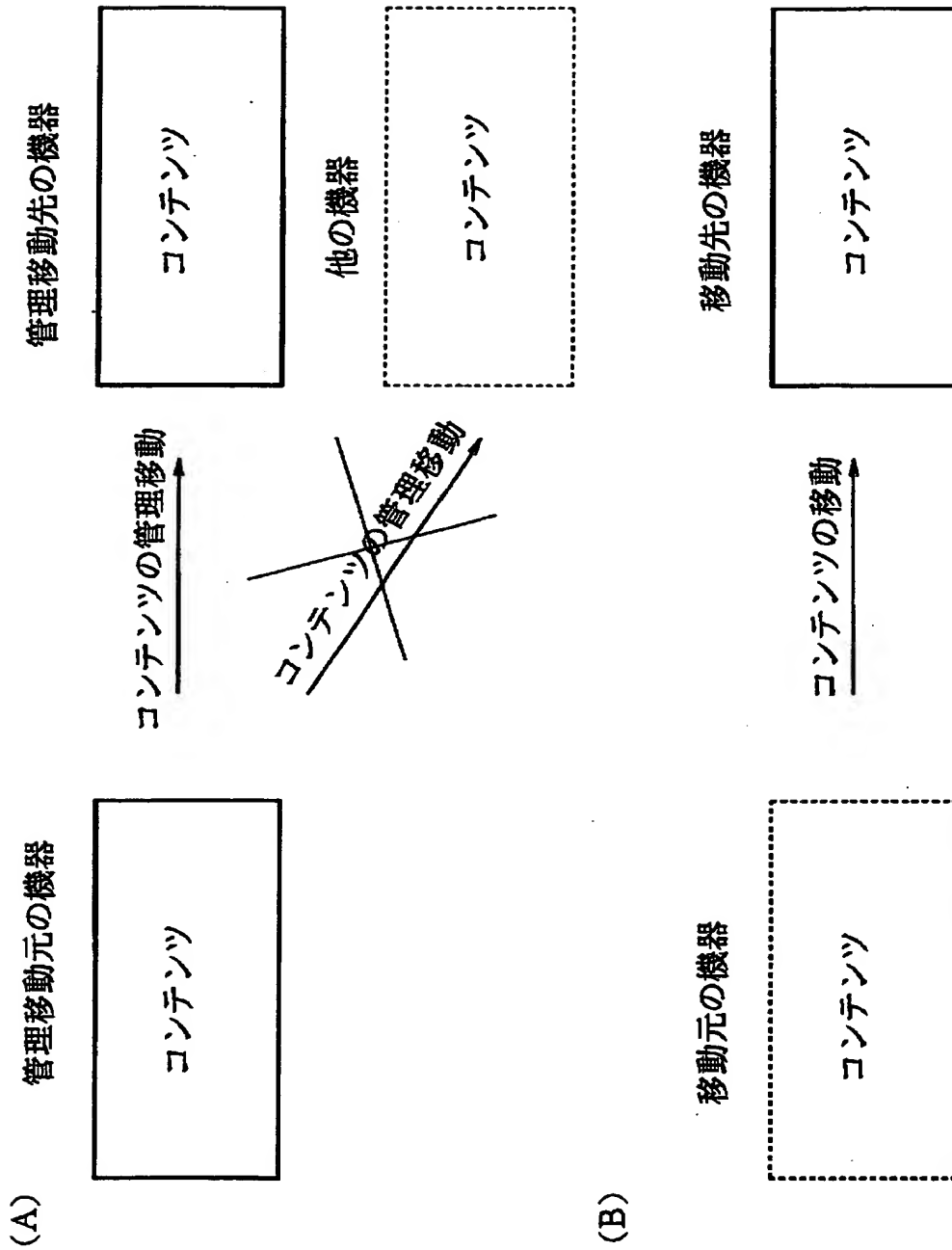
ucpB

(A)

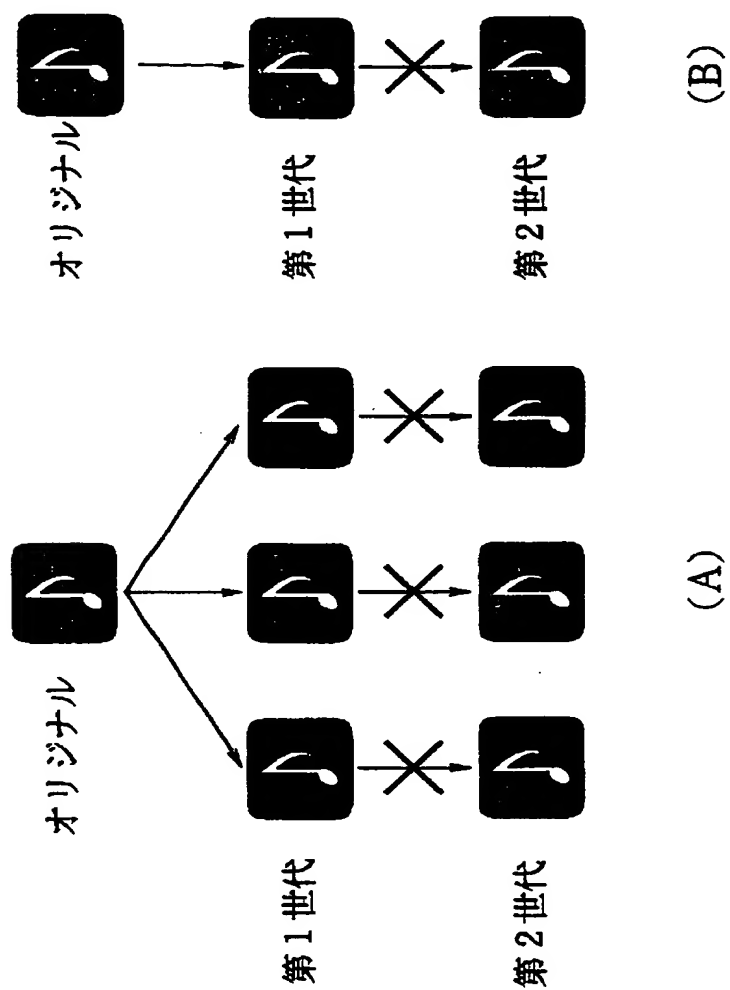
コンテンツの ID	コンテンツ A の ID
コンテンツプロバイダの ID	コンテンツプロバイダ 2 の ID
UCP の ID	ucpA の ID
UCP の有効期限	ucpA の有効期限
利用条件 10	ユーザ条件 10
	機器条件 10
利用内容 11	ID 11
	形式 11
	パラメータ 11
	管理移動許可情報 11
利用内容 12	ID 12
	形式 12
	パラメータ 12
	管理移動許可情報 12
利用内容 13	ID 13
	形式 13
	パラメータ 13
	管理移動許可情報 13
利用内容 14	ID 14
	形式 14
	パラメータ 14
	管理移動許可情報 14

ucpA

【図 1 0】



【図 11】



【図 12】

(A)

サービスコード	意 味
0000h	条件なし
0001h 乃至 00FFh	機器に関し条件有り
0100h 乃至 01FFh	性別条件あり
0200h 乃至 02FFh	年齢条件あり
0300h 乃至 7FFFh	その他の条件あり
8000h 乃至 FFFFh	利用ポイントに関し条件有り

(B)

コンディションコード	意 味
00h	無条件
01h	=
02h	≠
03h	<(より小さい)
04h	>(より大きい)
05h	≤(以下)
06h	≥(以上)
07h 乃至 FFh	空き

【図 13】

(A)

ユーザ条件 10	サービスコード	バリュースコード	コンディションコード
	80××h	0000C8h	06h
機器条件 10	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

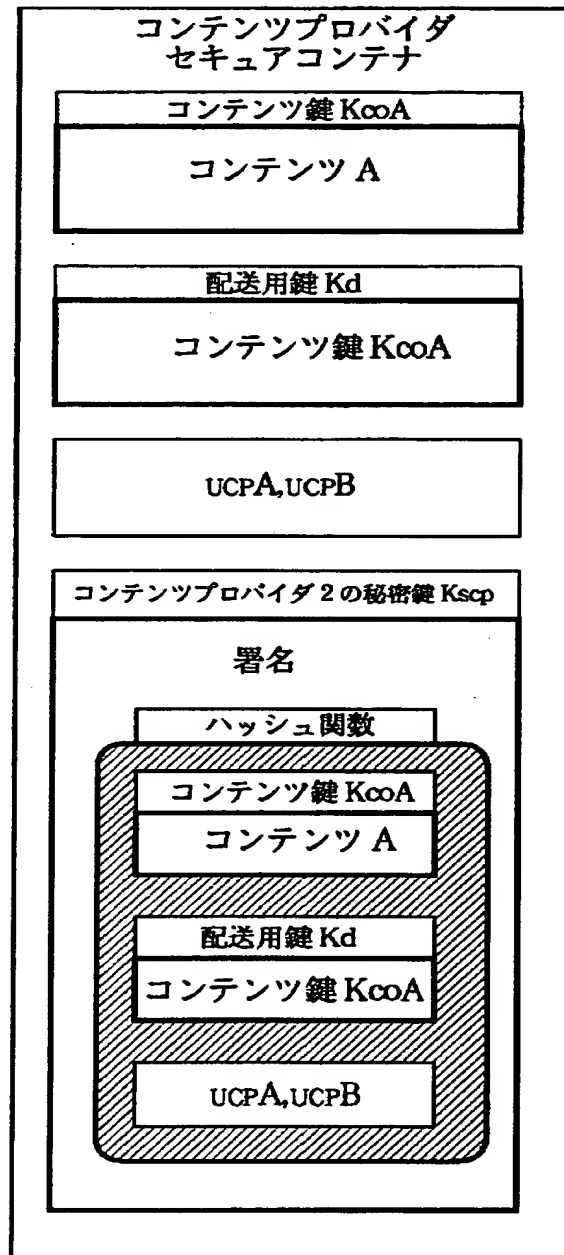
UCPA の利用条件 10

(B)

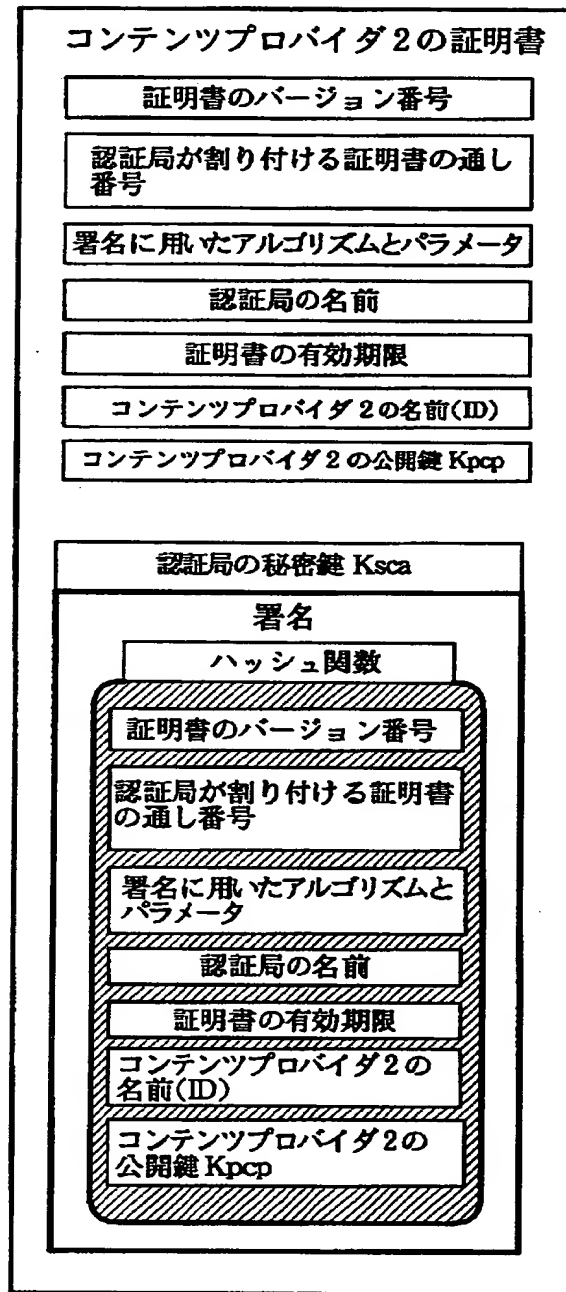
ユーザ条件 20	サービスコード	バリュースコード	コンディションコード
	80××h	0000C8h	03h
機器条件 20	サービスコード	バリュースコード	コンディションコード
	0000h	FFFFFFh	00h

UCPB の利用条件 20

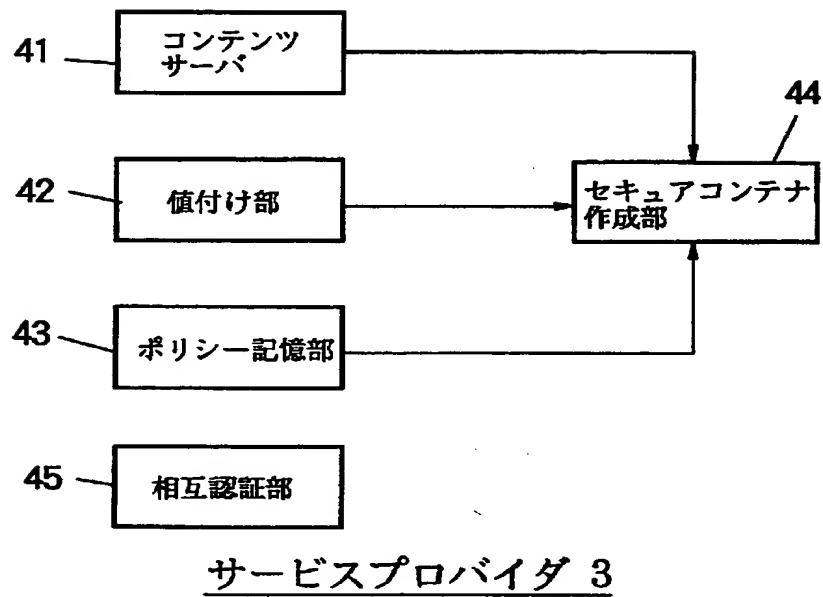
【図 14】



【図 15】



【図 16】



【図 1 7】

コンテンツの ID	コンテンツ A の ID	
コンテンツ プロバイダの ID	コンテンツプロバイダ 2 の ID	
UCP の ID	ucpA の ID	
UCP の有効期限	ucpA の有効期限	
サービス プロバイダの ID	サービスプロバイダ 3 の ID	
PT の ID	ptA-2 の ID	
PT の有効期限	ptA-2 の有効期限	
価格条件 20	ユーザ条件 20	女性
	機器条件 20	条件なし
価格内容 21	1000 円	
価格内容 22	300 円	
価格内容 23	50 円	
価格内容 24	150 円	

PTA-2

コンテンツの ID	コンテンツ A の ID		
コンテンツ プロバイダの ID	コンテンツプロバイダ 2 の ID		
UCP の ID	ucpA の ID		
UCP の有効期限	ucpA の有効期限		
サービス プロバイダの ID	サービスプロバイダ 3 の ID		
PT の ID	ptA-1 の ID		
PT の有効期限	ptA-1 の有効期限		
価格条件 10	ユーザ条件 10	男性	
	機器条件 10	条件なし	
価格内容 11	2000 円		
価格内容 12	600 円		
価格内容 13	100 円		
価格内容 14	300 円		

PTA-1

【図 18】

(A)

ユーザ 条件 10	サービスコード	バリューコード	コンディションコード
	01××h	000000h	01h
機器条件 10	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-1 の価格条件 10

(B)

ユーザ 条件 20	サービスコード	バリューコード	コンディションコード
	01××h	000001h	01h
機器 条件 20	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h

PTA-2 の価格条件 20

【図 1 9】

コンテンツの ID	コンテンツ A の ID
コンテンツ プロバイダの ID	コンテンツプロバイダ 2 の ID
UCP の ID	ucpB の ID
サービス プロバイダの ID	サービスプロバイダ 3 の ID
PT の ID	PTB-2 の ID
PT の有効期限	PTB-2 の有効期限
価格条件 40	ユーザ条件 40
	条件なし
価格内容 41	機器条件 40
	主機器
価格内容 42	50 円
	150 円

PTB-2

(B)

コンテンツの ID	コンテンツ A の ID
コンテンツ プロバイダの ID	コンテンツプロバイダ 2 の ID
UCP の ID	ucpB の ID
サービス プロバイダの ID	サービスプロバイダ 3 の ID
PT の ID	PTB-1 の ID
PT の有効期限	PTB-1 の有効期限
価格条件 30	ユーザ条件 30
	条件なし
価格内容 31	機器条件 30
	従機器
価格内容 32	100 円
	300 円

PTB-1

(A)

【図 20】

(A)

ユーザ条件 30	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 30	サービスコード	バリューコード	コンディションコード
	00××h	000064h	03h

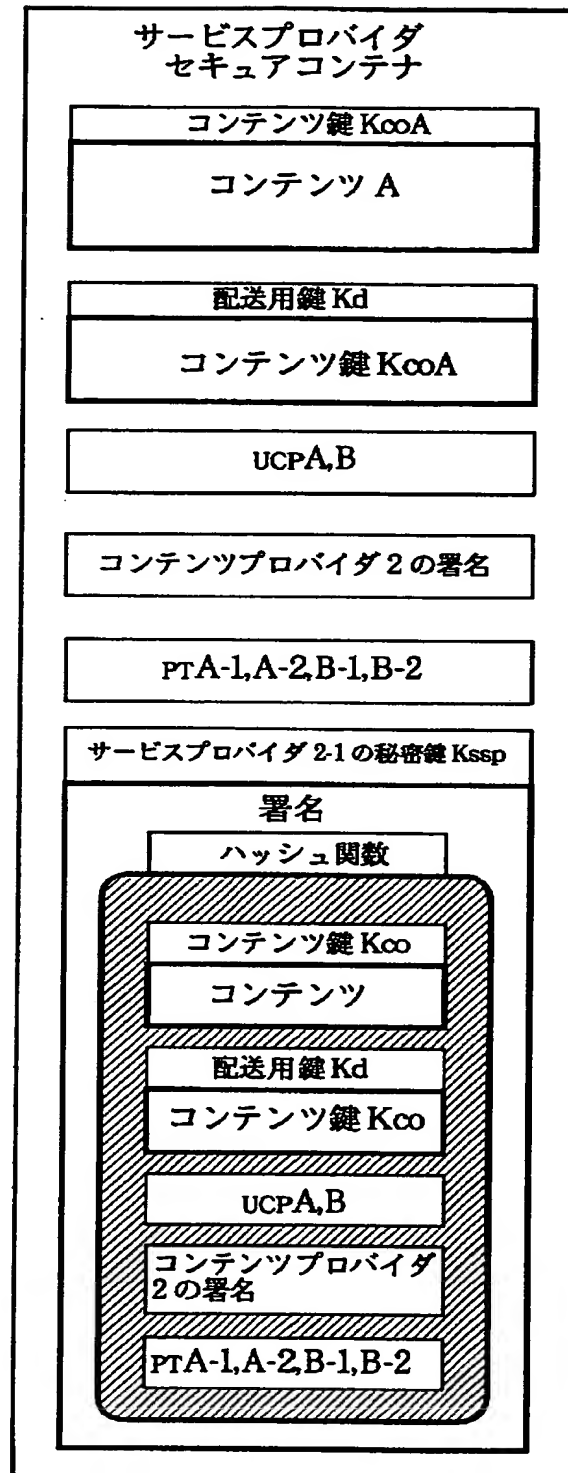
PTB-1 の価格条件 30

(B)

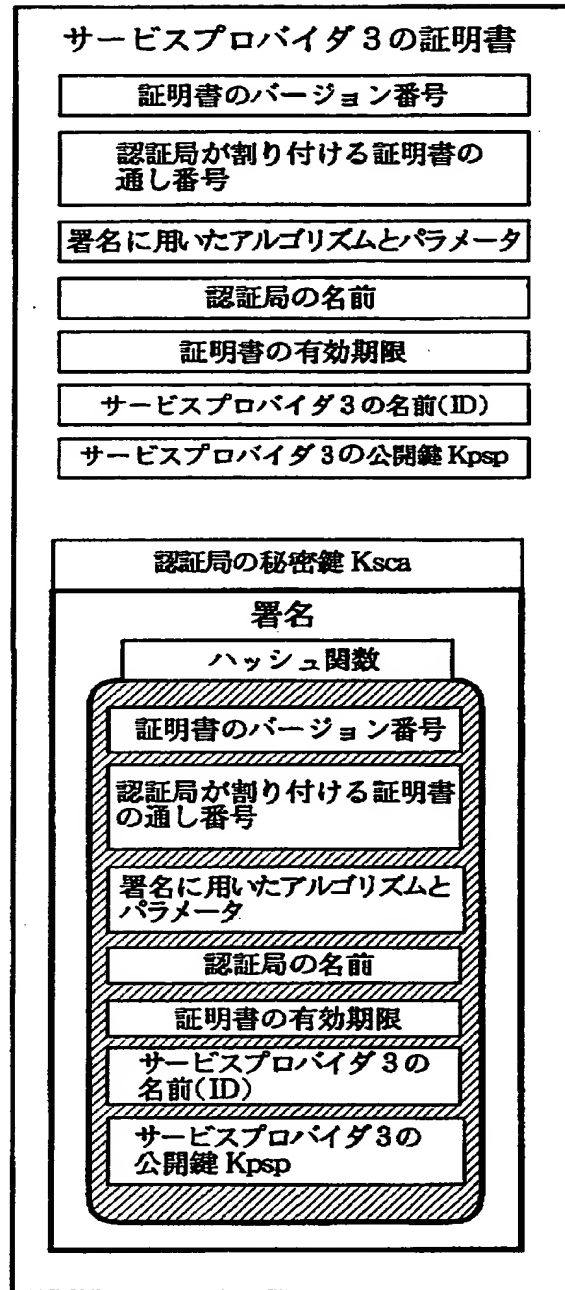
ユーザ条件 40	サービスコード	バリューコード	コンディションコード
	0000h	FFFFFFh	00h
機器条件 40	サービスコード	バリューコード	コンディションコード
	00××h	000064h	06h

PTB-2 の価格条件 40

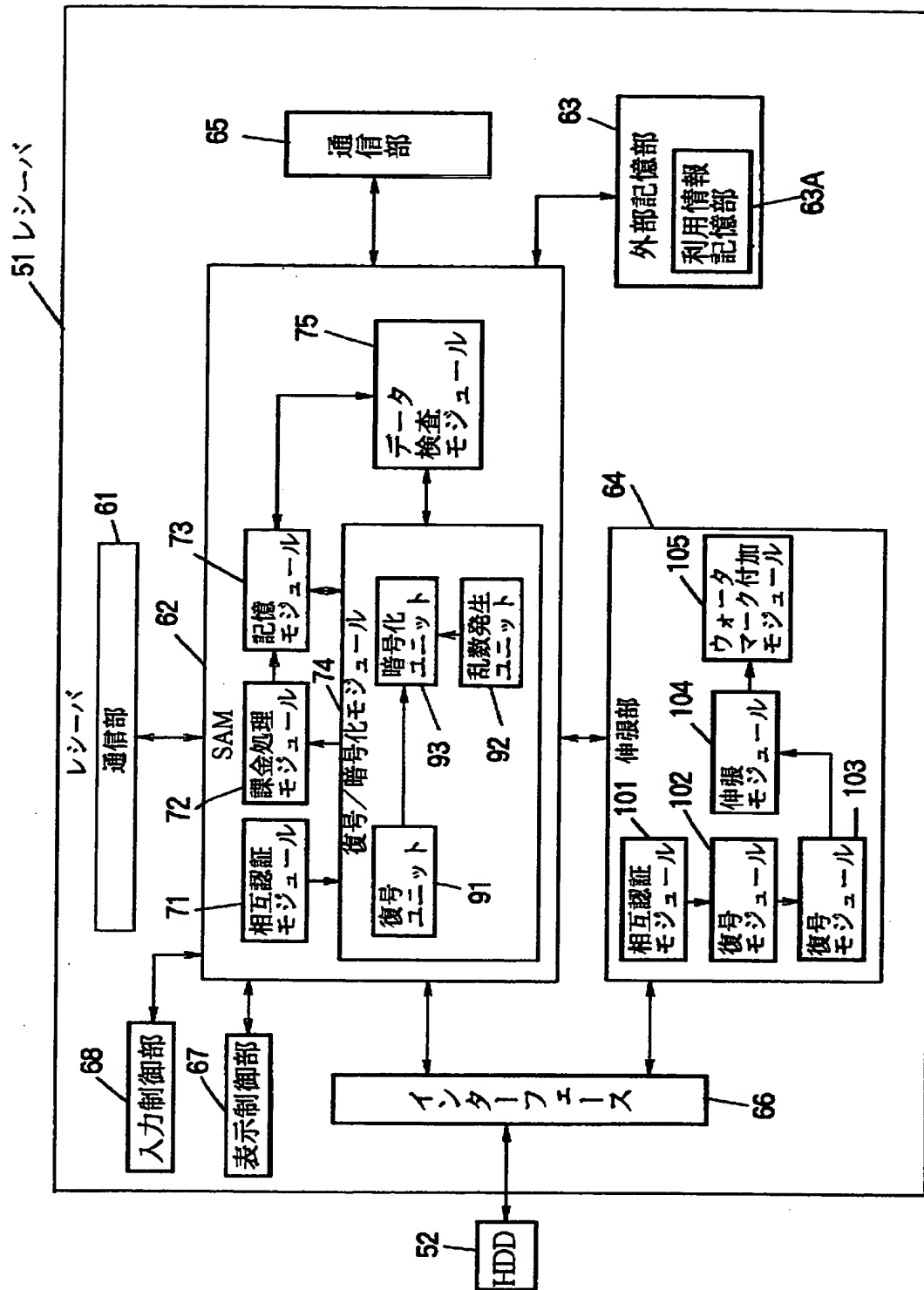
【図 21】



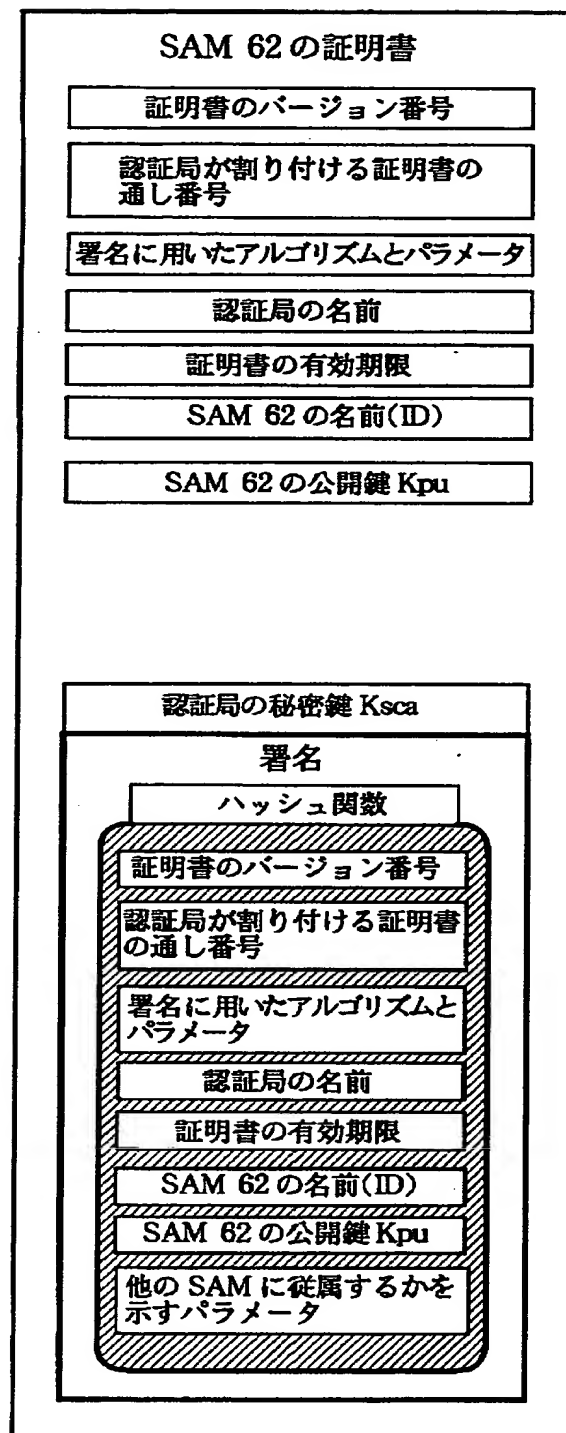
【図 22】



【図 23】



【図 24】

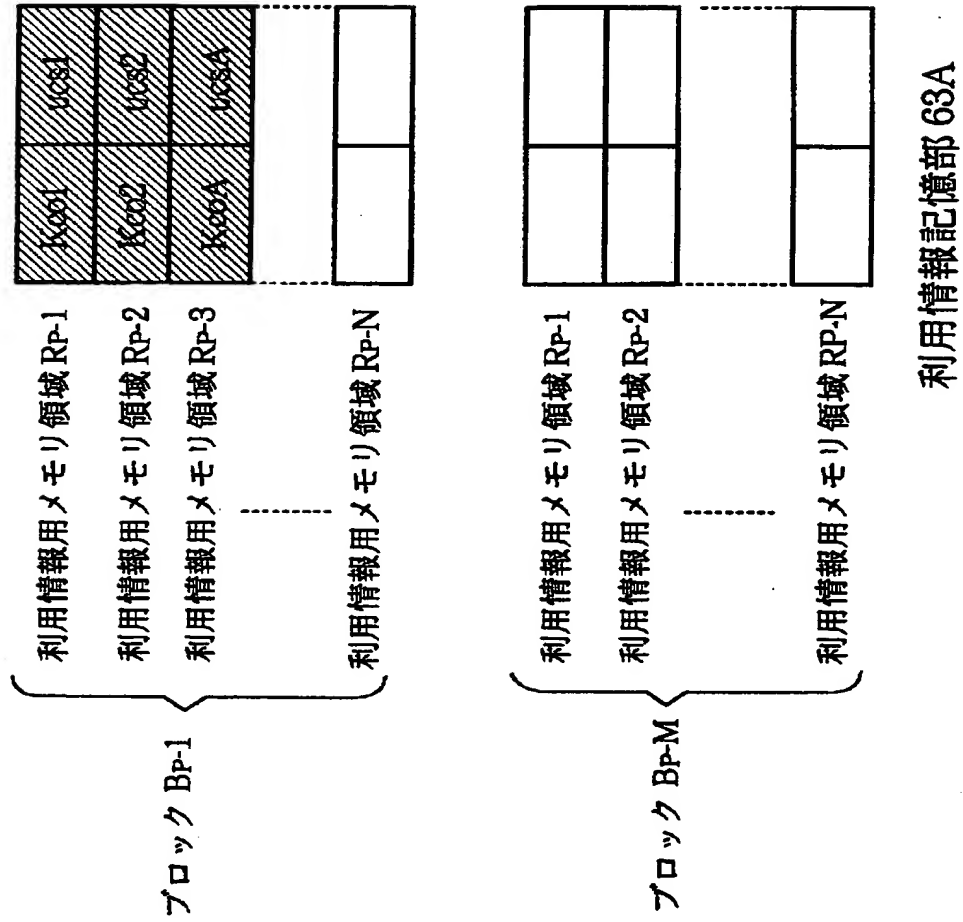


【図 25】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		UCPA の ID
UCP の有効期限		UCPA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		PTA-1 の ID
PT の有効期限		PTA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 11 の ID
	形式	買い取り再生
	パラメータ	× × ×
	管理移動 状態情報	管理移動元 : SAM62 の ID、 管理移動先 : SAM62 の ID
利用履歴		× × ×

ucsA

【図 2 6】



【図 27】

コンテンツの ID		コンテンツ A の ID
コンテンツ プロバイダの ID		コンテンツプロバイダ 2 の ID
UCP の ID		ucpA の ID
UCP の有効期限		ucpA の有効期限
サービス プロバイダの ID		サービスプロバイダ 3 の ID
PT の ID		ptA-1 の ID
PT の有効期限		ptA-1 の有効期限
UCS の ID		ucsA の ID
SAM の ID		SAM62 の ID
ユーザの ID		ユーザ F の ID
利用 内容	ID	利用内容 11 の ID
	形式	買い取り再生
	パラメータ	×××
	管理移動 状態情報	管理移動元：SAM62 の ID、 管理移動先：SAM62 の ID
課金履歴		×××

課金情報 A

【図 28】

SAM62 の公開鍵 Kpu	
SAM62 の秘密鍵 Ksu	
EMD サービスセンタ 1 の公開鍵 Kpesc	
認証局の公開鍵 Kpca	
保存用鍵 Ksave	
3 月分の配送用鍵 Kd	
⋮	
SAM62 の証明書	
基準情報 51	
課金情報	
⋮	
検査値 Hp-1	検査値 Hp-2
⋮	
検査値 Hp-M	

【図 29】

SAM の ID		SAM62 の ID
機器番号		レシーバ 51 の機器番号 (100 番)
決済 ID		ユーザの決済 ID
課金の上限額		正式登録時の課金の 上限額
決済 ユーザ 情報	氏名	ユーザの氏名
	住所	ユーザの住所
	電話番号	ユーザの電話番号
	決済機関情報	ユーザの決済機関情報
	生年月日	ユーザの生年月日
	年齢	ユーザの年齢(21 才)
	性別	ユーザの性別(男)
	ユーザの ID	ユーザの ID
	パスワード	ユーザのパスワード

利用ポイント情報	レシーバ 51 の利用 ポイント情報
----------	-----------------------

基準情報 51

【図 30】

レシーバ
51 の登録
条件

レシーバ
201 の登録
条件

SAM ID	ユーザ ID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ	登録条件 署名	登録リス ト署名
SAM62 の ID	ユーザの ID	可	可	SAM62 の ID	なし	制限 なし	××××	××××
SAM212 の ID	ユーザの ID	可	不可	SAM62 の ID	なし	制限 なし	××××	

リスト部

対象 SAM ID

有効期限

バージョン番号

接続されている機器数

SAM62 の ID

××××

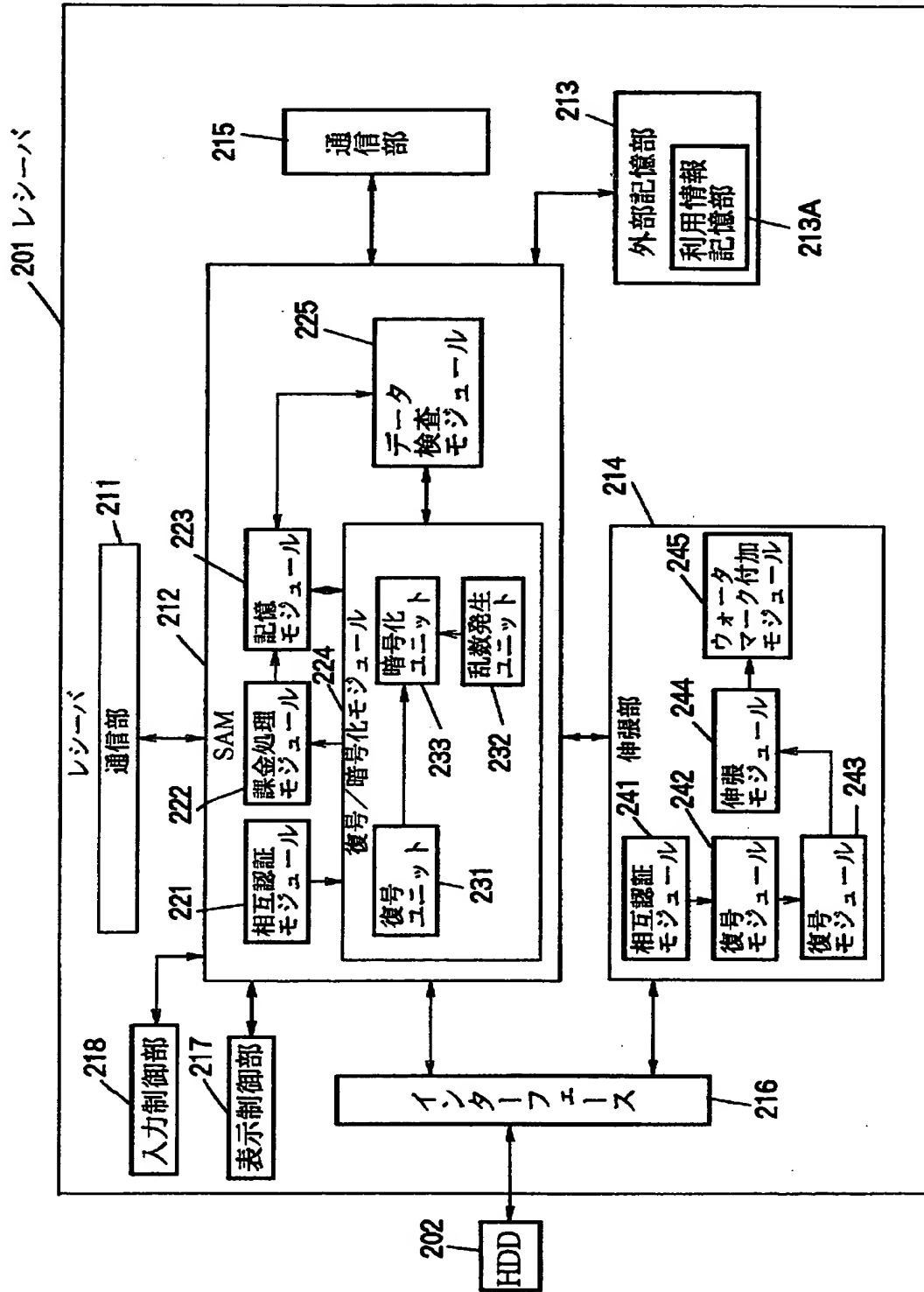
××××

2

対象 SAM 情報部

レシーバ 51 の登録リスト

【図 3 1】



【図 3 2】

リスト部

SAM ID	ユーザ ID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ	登録条件 署名	登録リス ト署名
レシーバ 51の登録 条件	SAM62の ユーザの ID	可	可	SAM62 のID	なし	制限 なし	XXXX	XXXX
レシーバ 201の登録 条件	SAM212の ユーザの ID	可	不可	SAM62 のID	なし	制限 なし	XXXX	

対象 SAM ID

SAM212 の ID

有効期限

XXXX

バージョン番号

XXXX

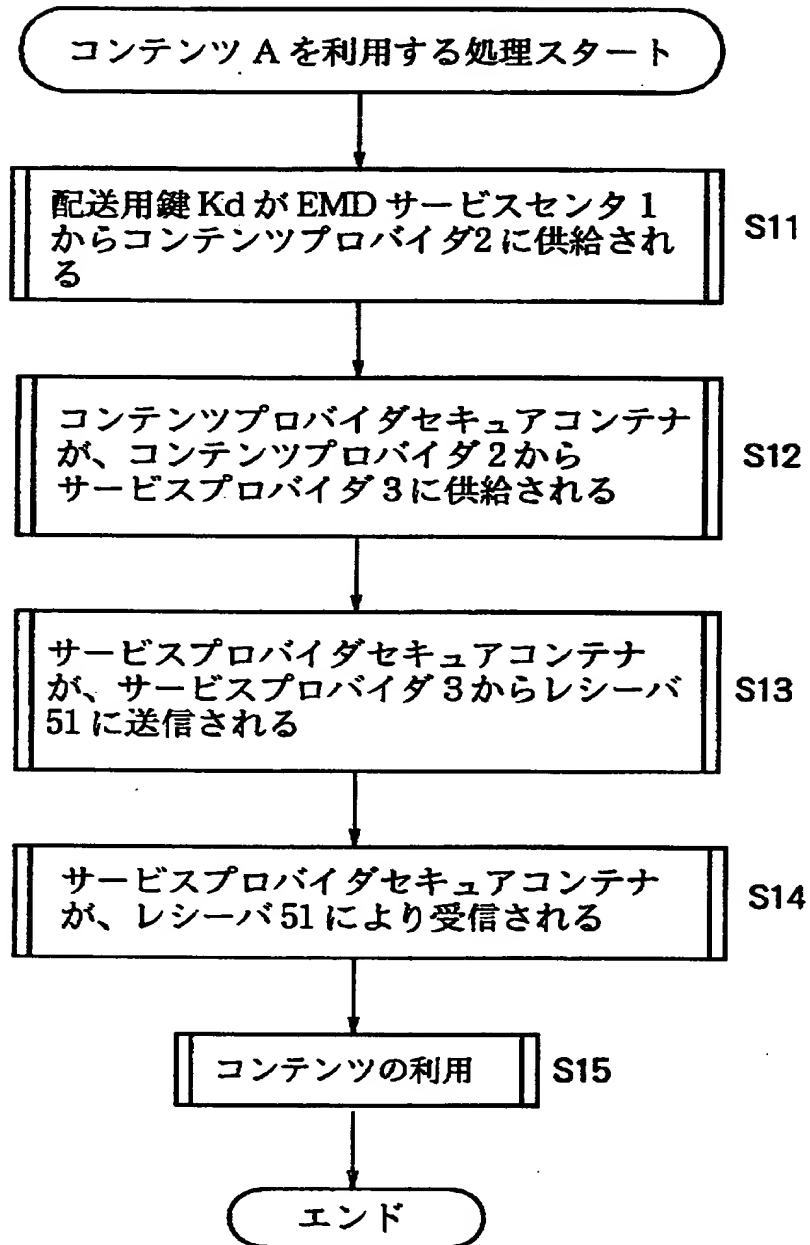
接続されている機器数

2

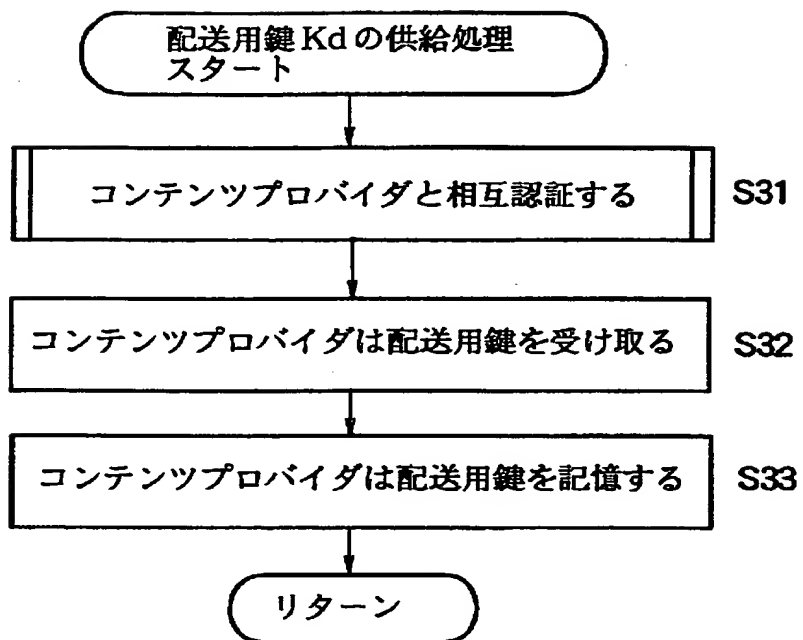
対象 SAM 情報部

レシーバ 201 の登録リスト

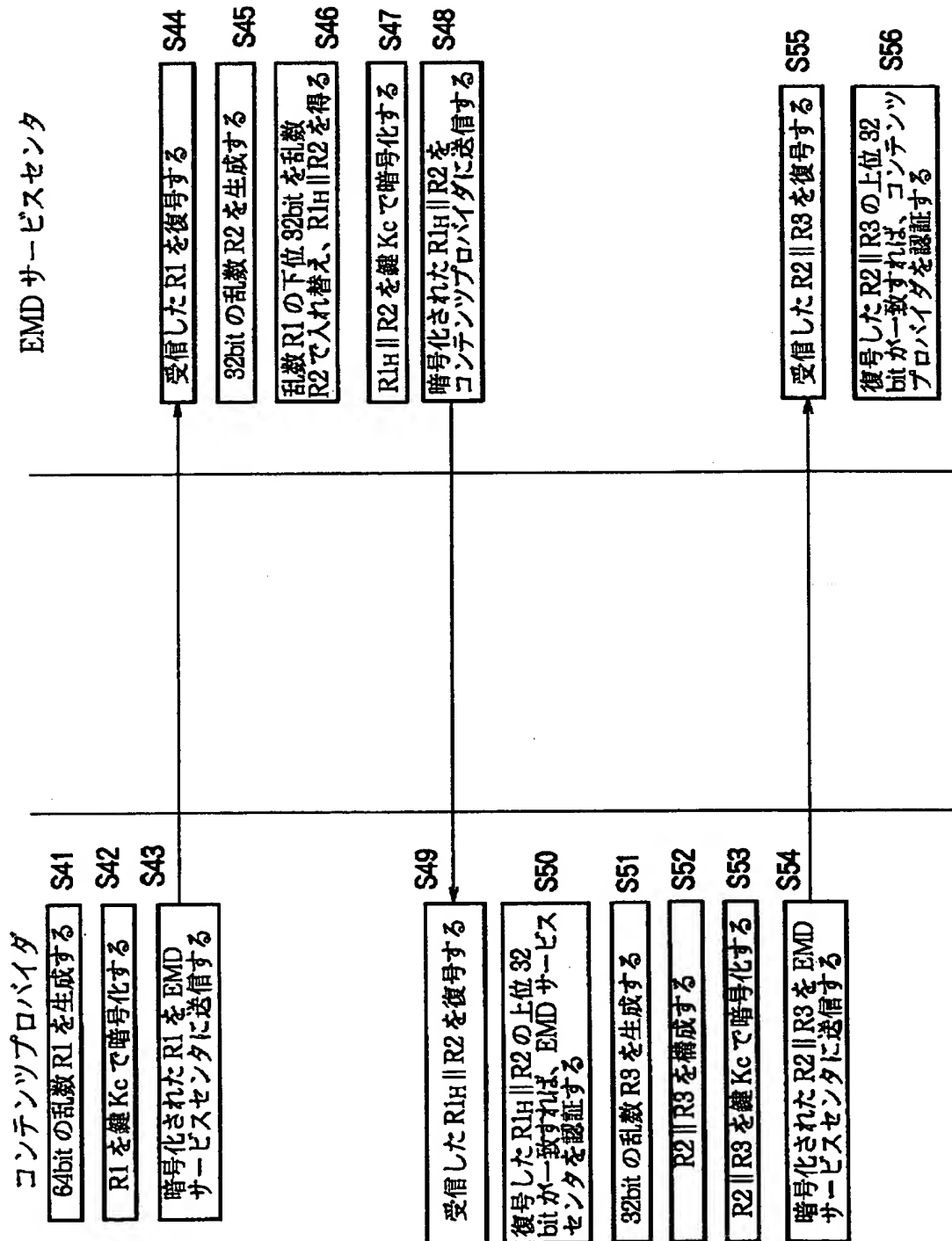
【図 33】



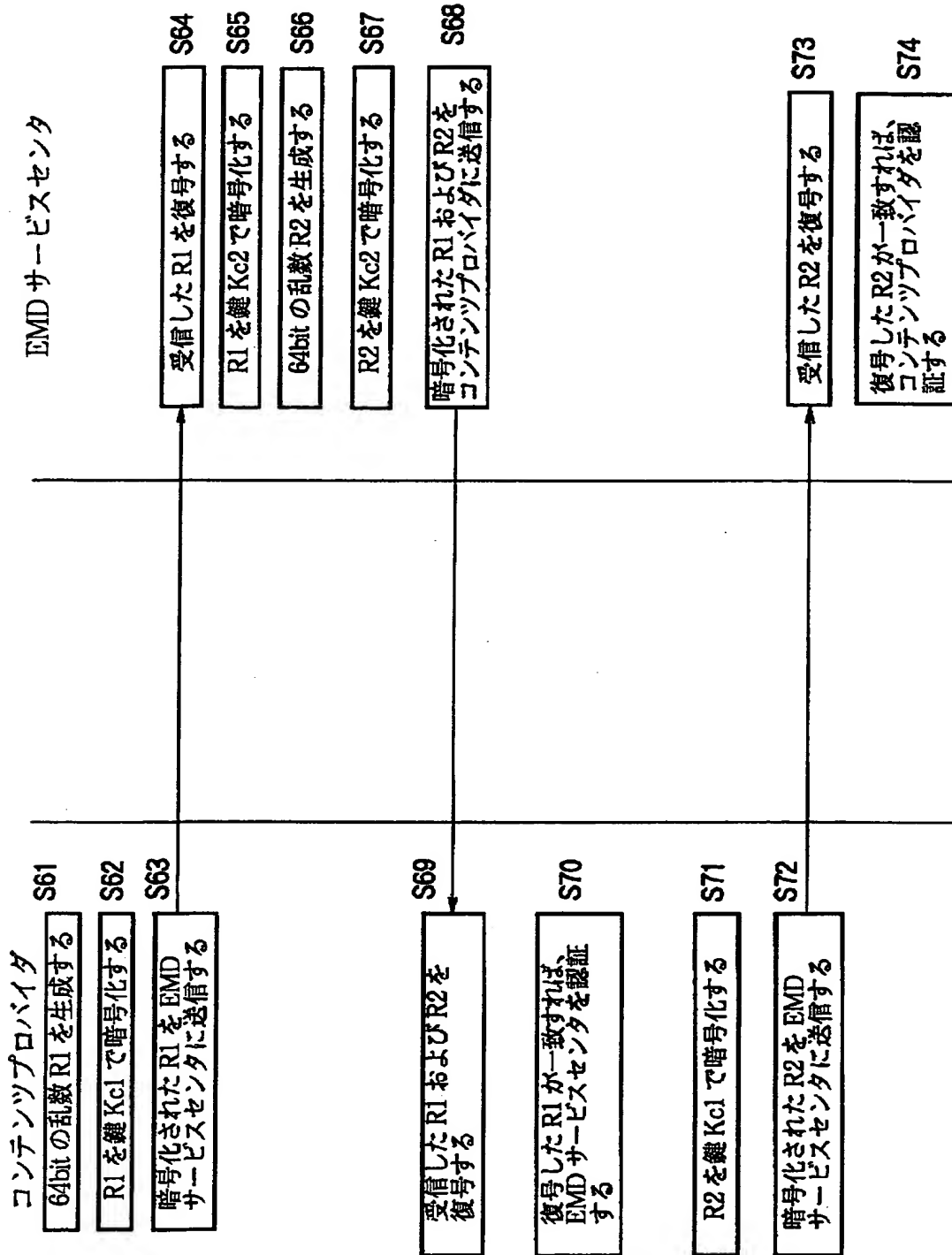
【図 3 4】



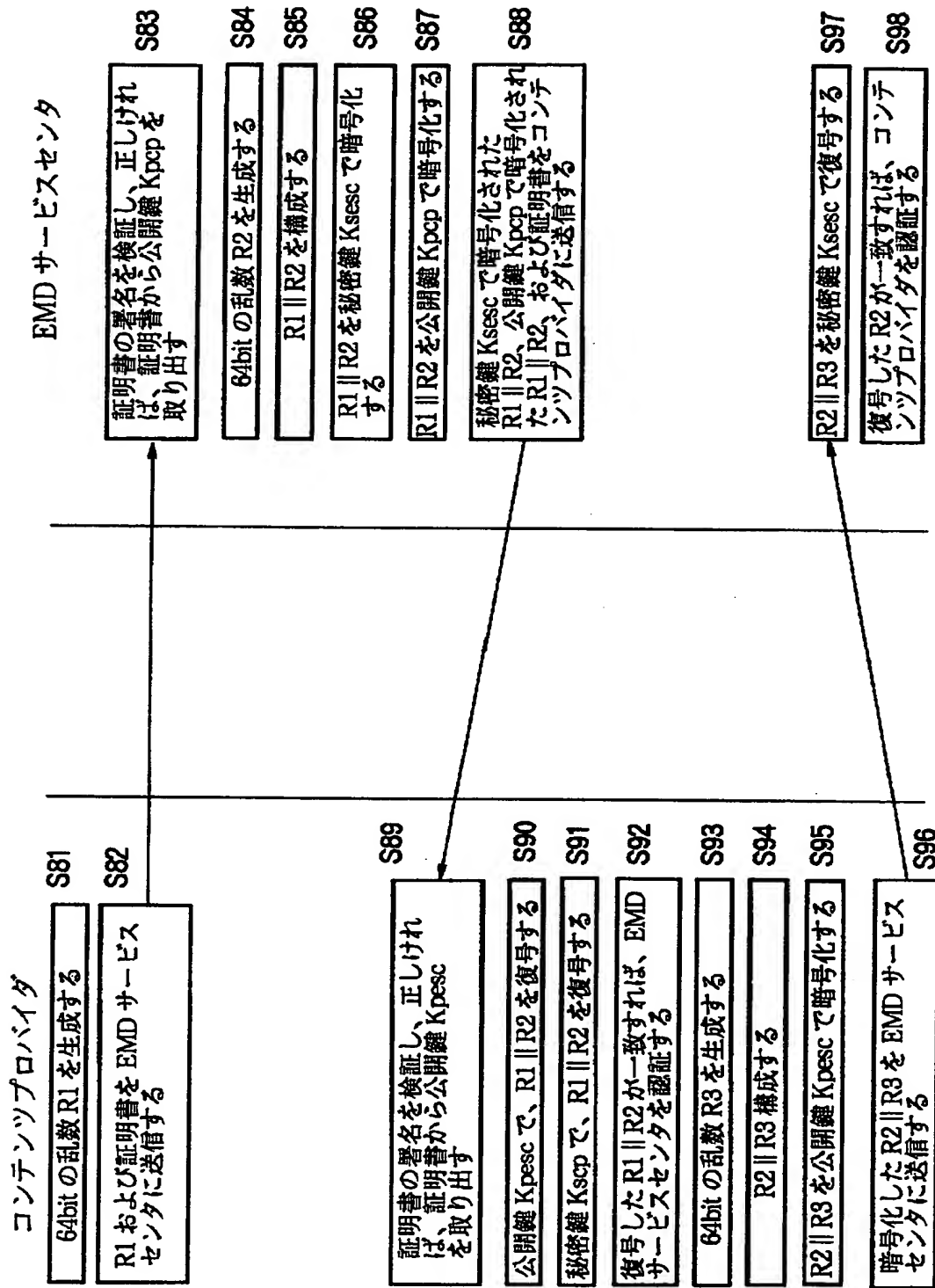
【図 3 5】



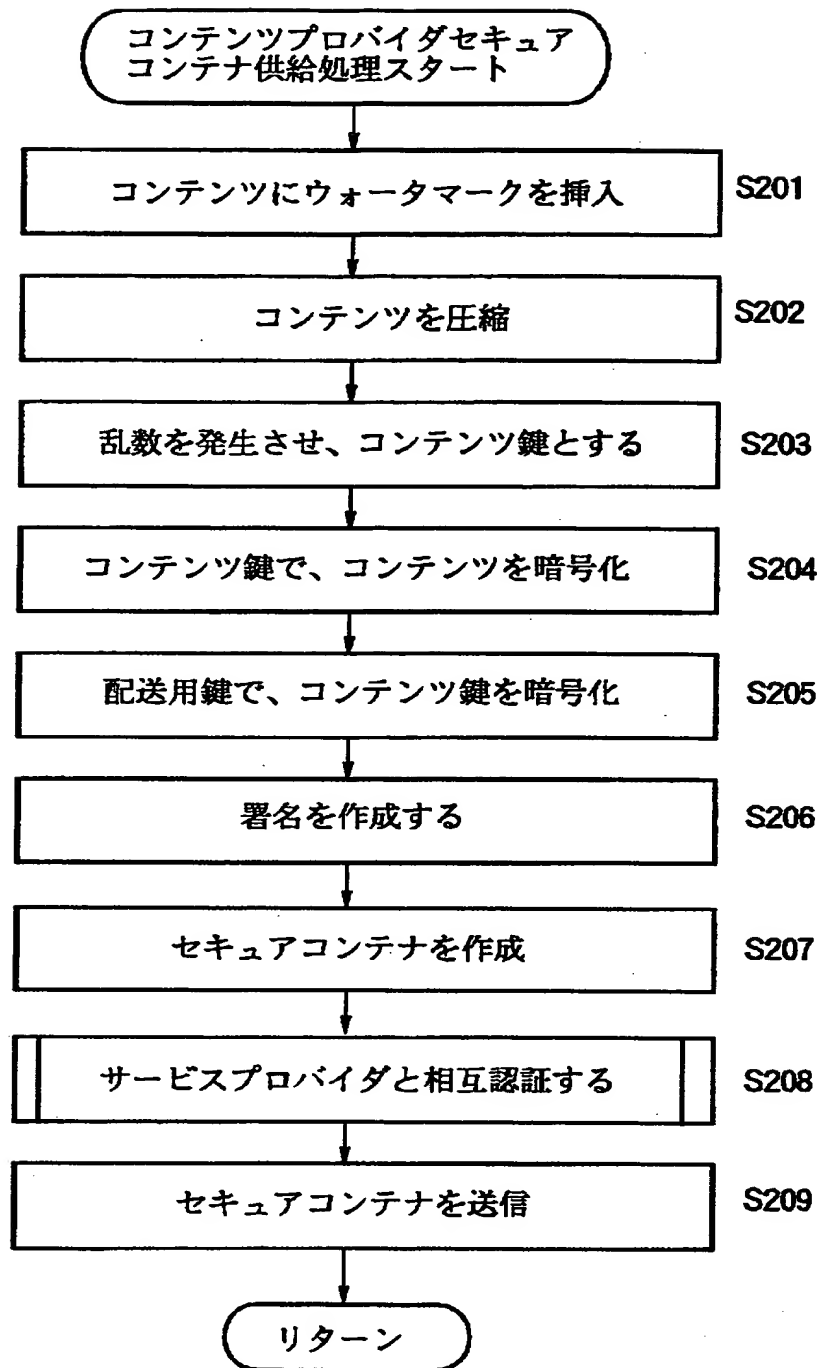
【図 3 6】



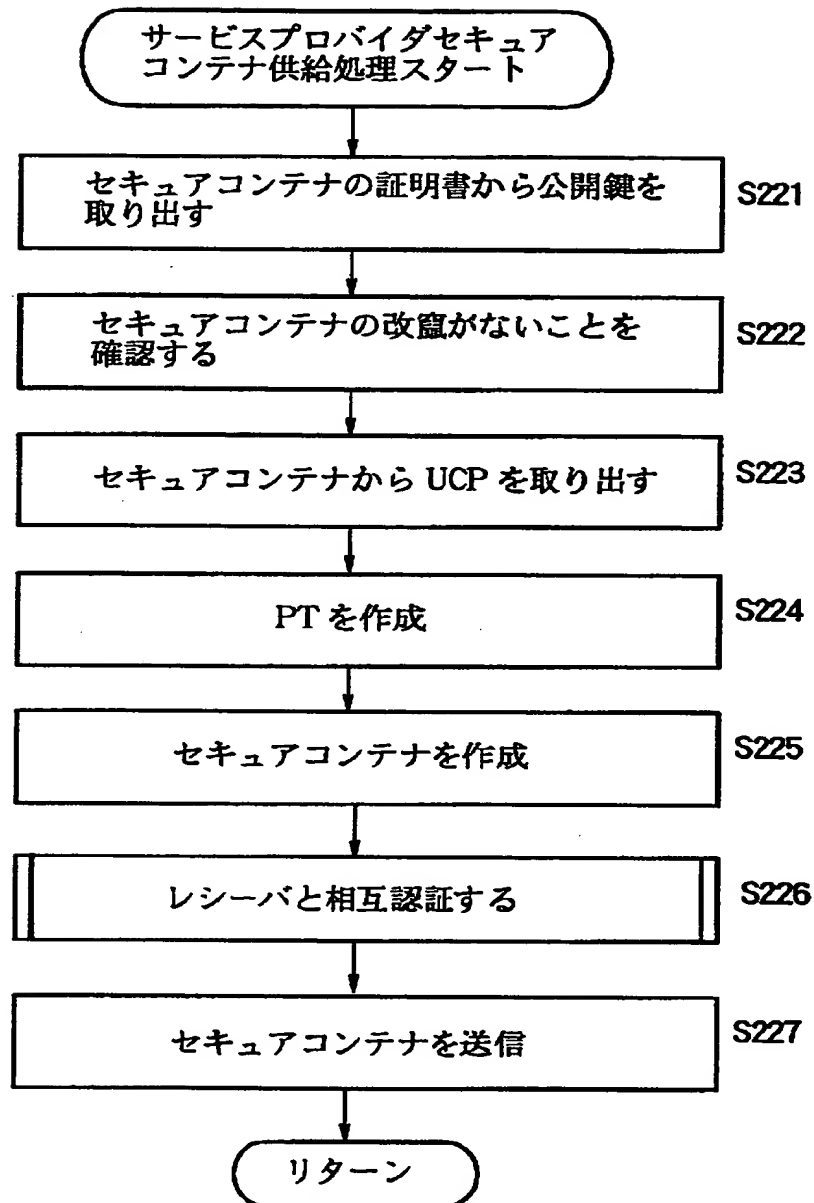
【図 3 7】



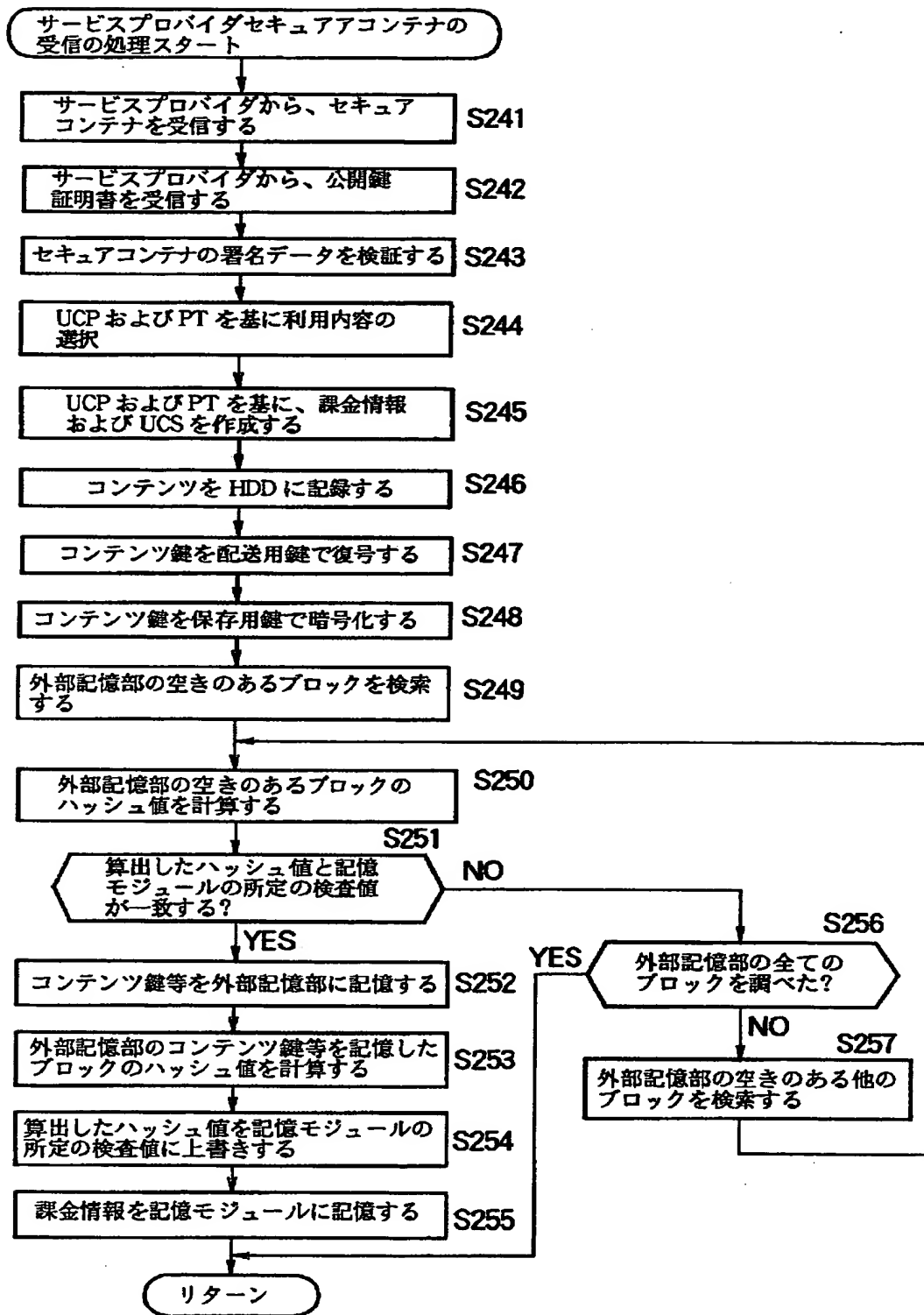
【図 38】



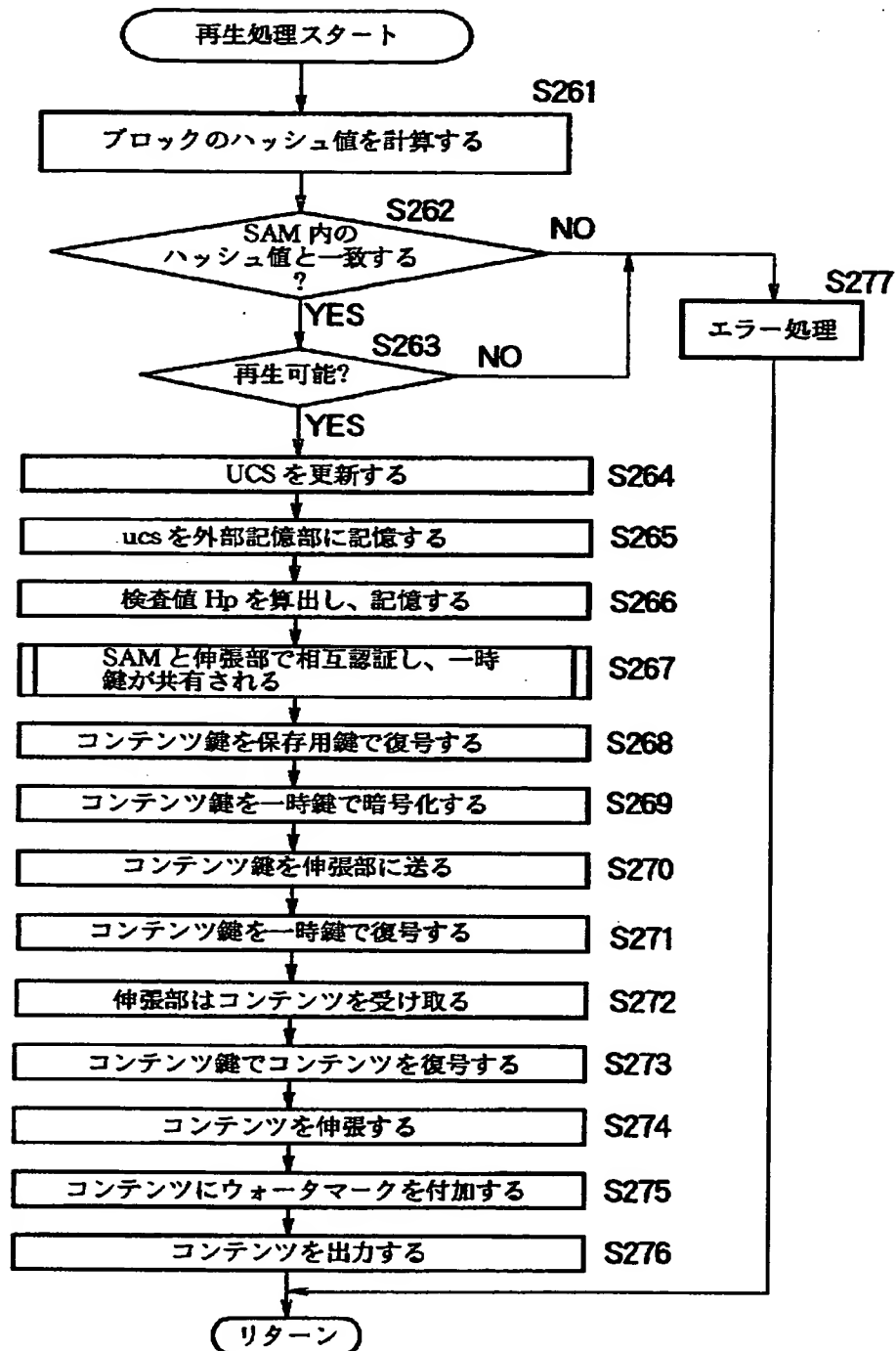
【図 39】



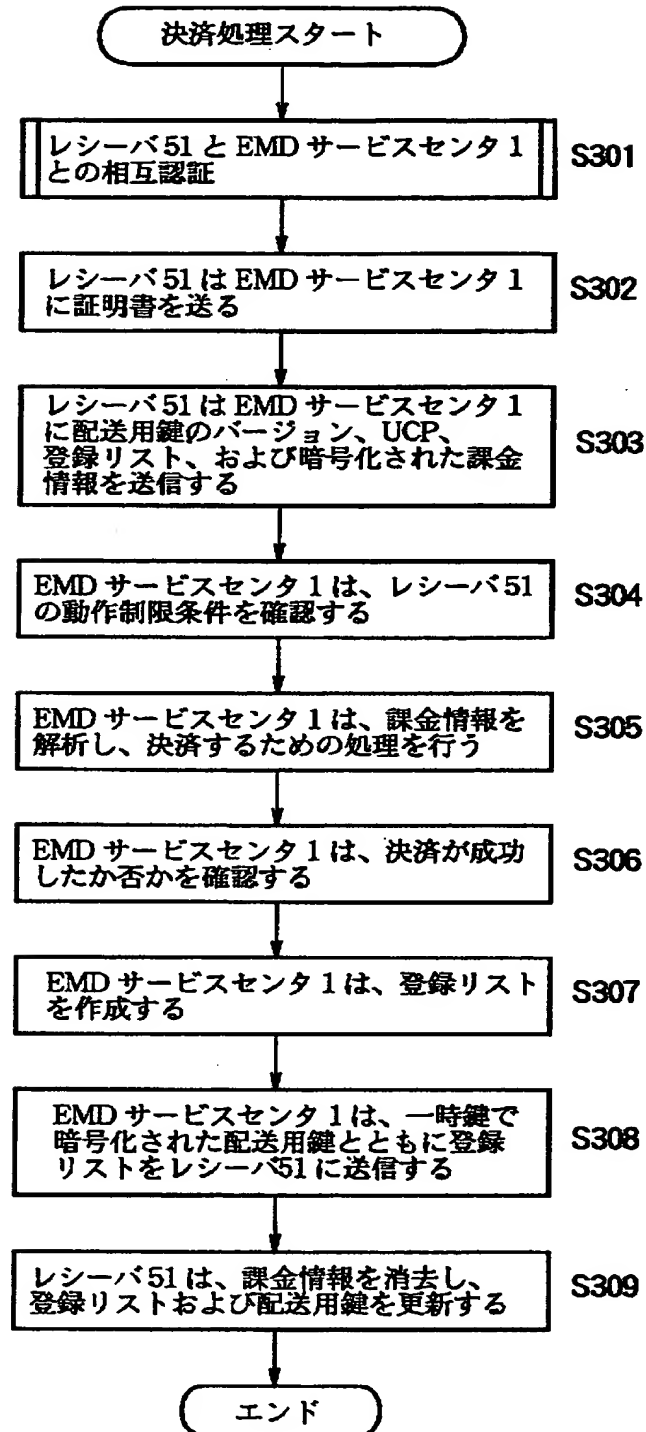
【図 40】



【図 4 1】

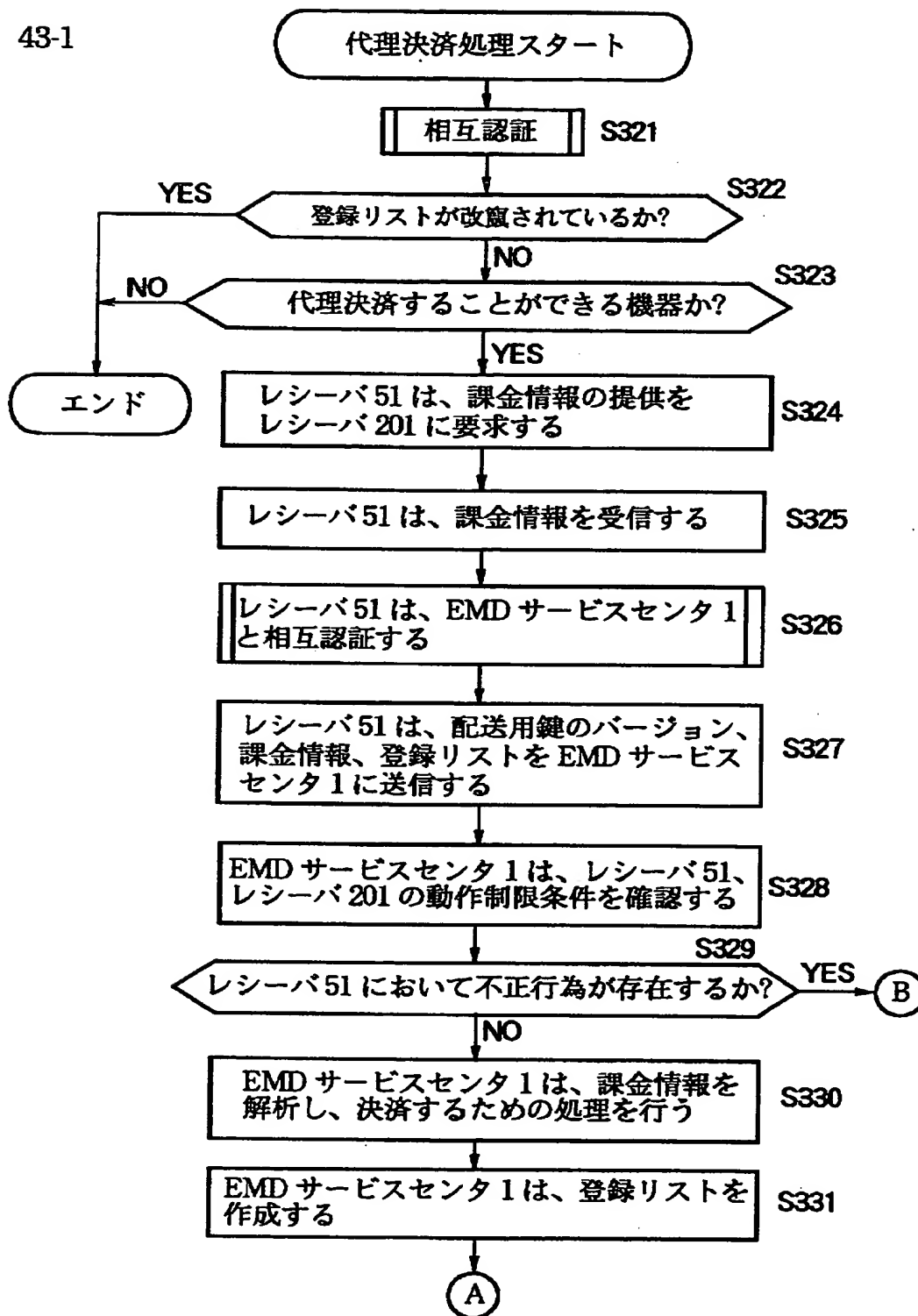


【図 4 2】



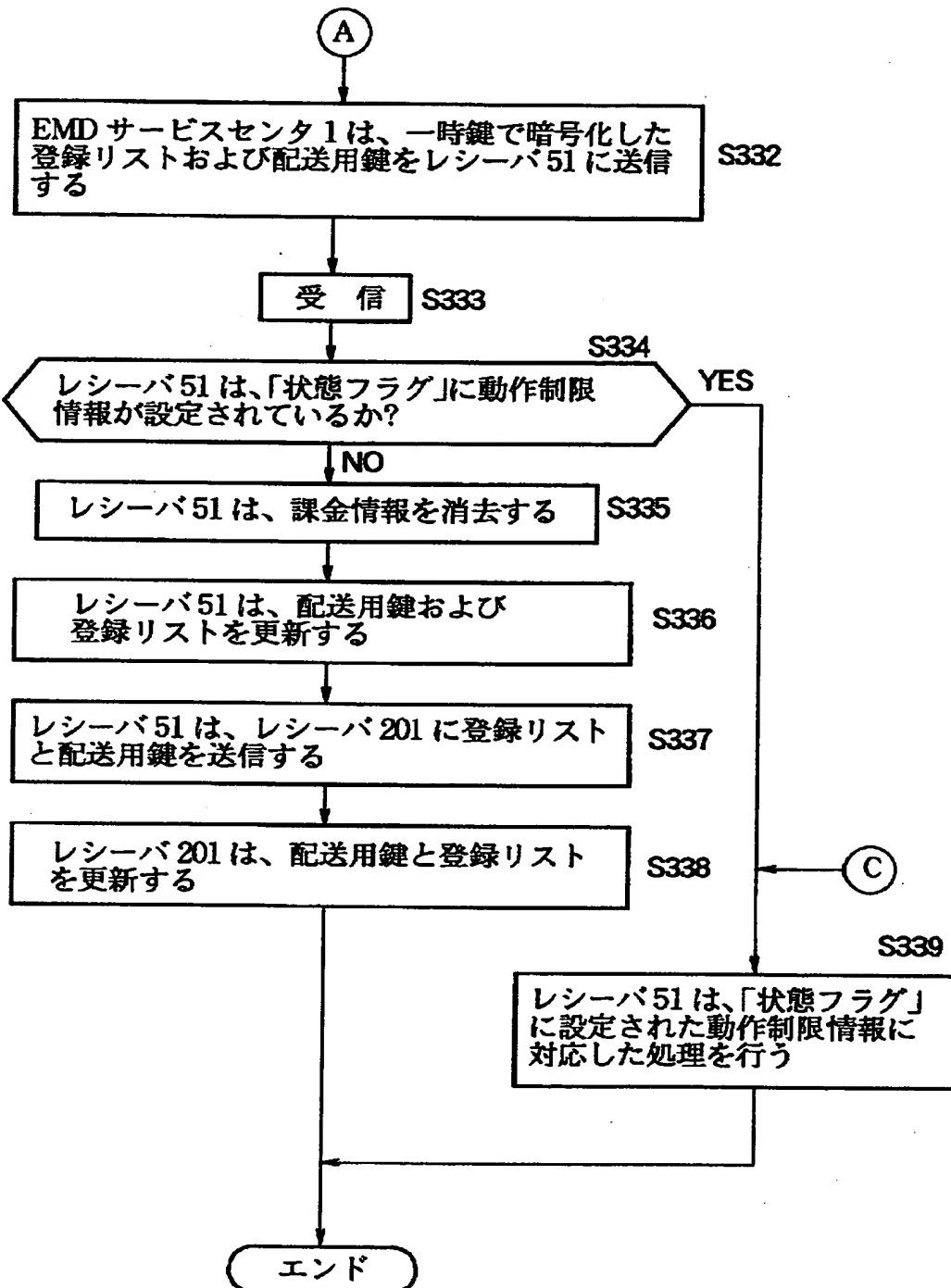
【図 4 3】

43-1



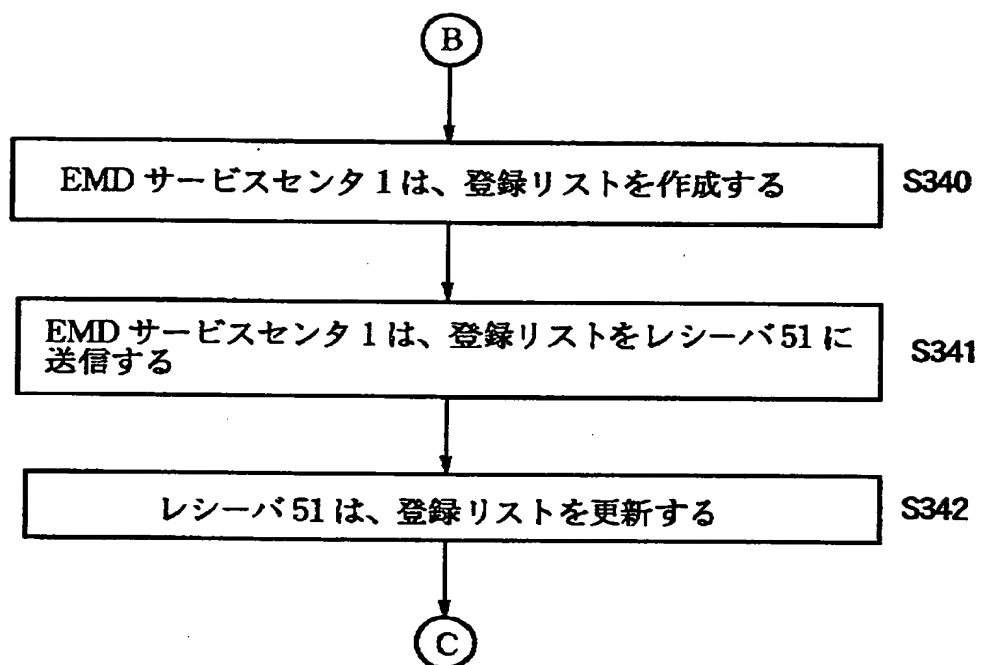
【図 4 4】

43-2

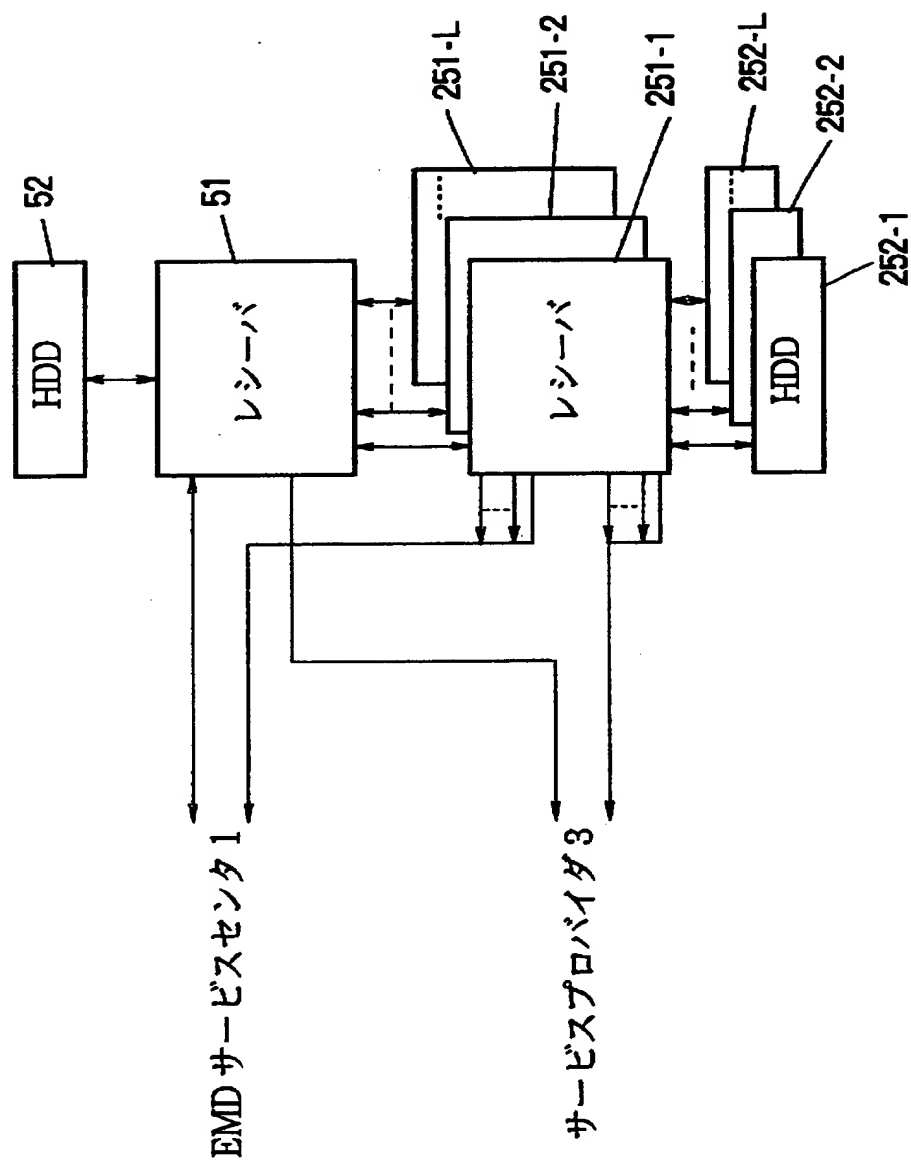


【図 4 5】

43-3



【図 4 6】



ユーザホームネットワーク 5

【図 4 8】

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リス ト署名	
レシーバ 51の登録 条件	SAM62の ユーザの ID	可	可	SAM62 の ID	なし	制限 なし	××××	××××	
レシーバ 251-1の 登録条件	SAMの ID ユーザの ID	可	不可	SAM62 の ID	なし	制限 なし	××××		
レシーバ 251-2の 登録条件	SAMの ID ユーザの ID	可	不可	SAM62 の ID	なし	制限 なし	××××		

レシーバ 251-1 の SAM の ID
××××

有効期限
××××

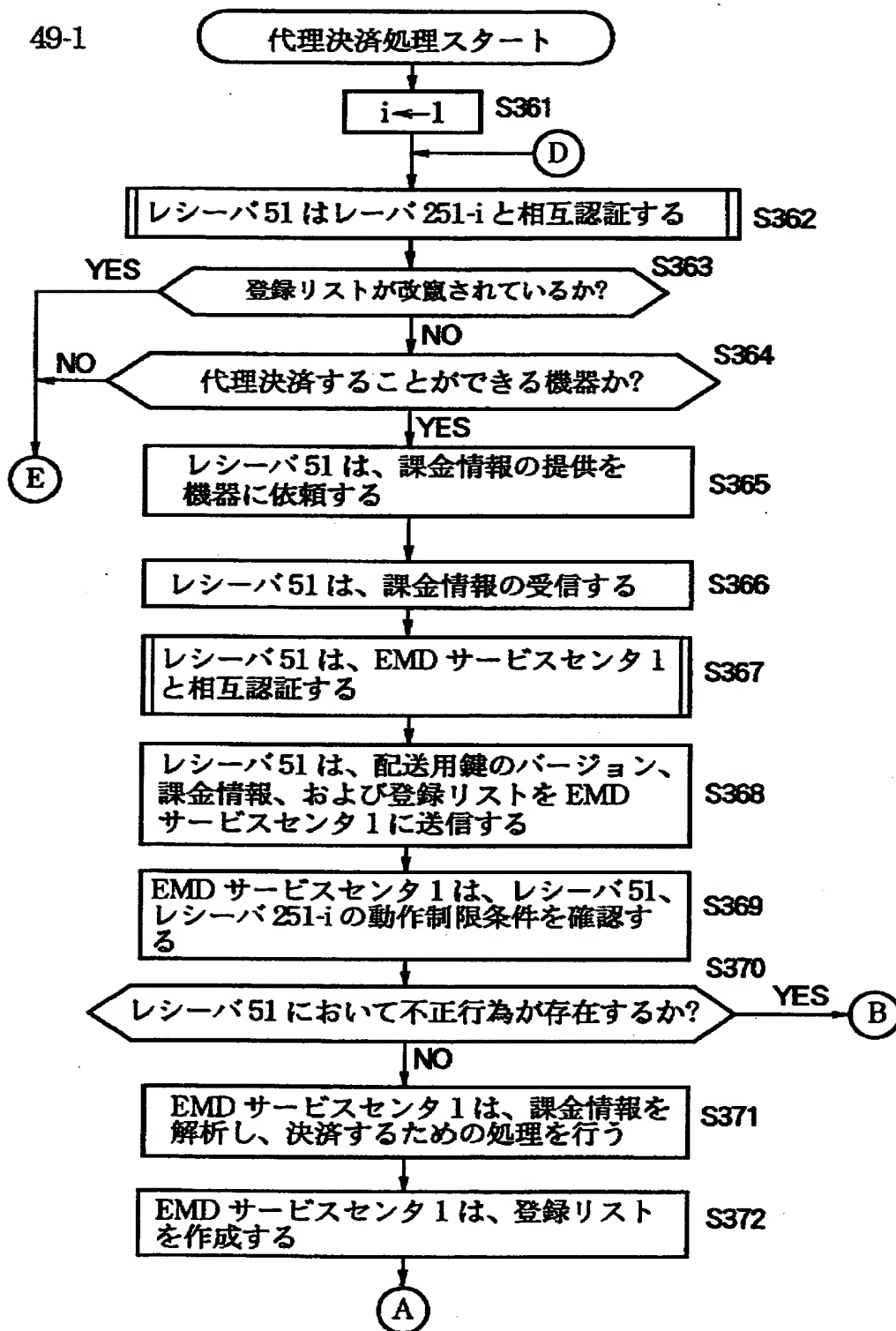
対象 SAM ID
××××

バージョン番号
2

対象 SAM 情報部

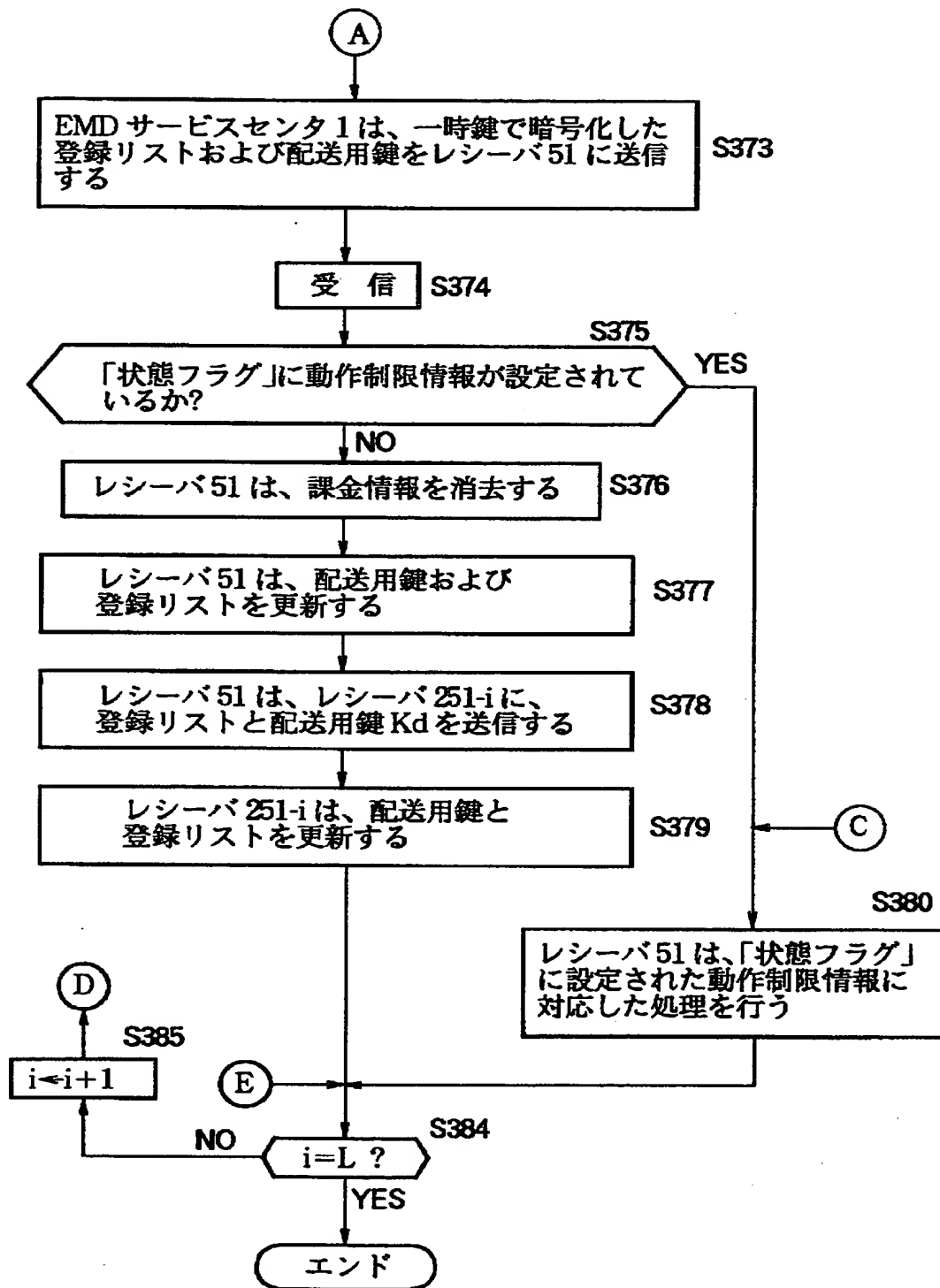
接続されている機器数

【図 49】

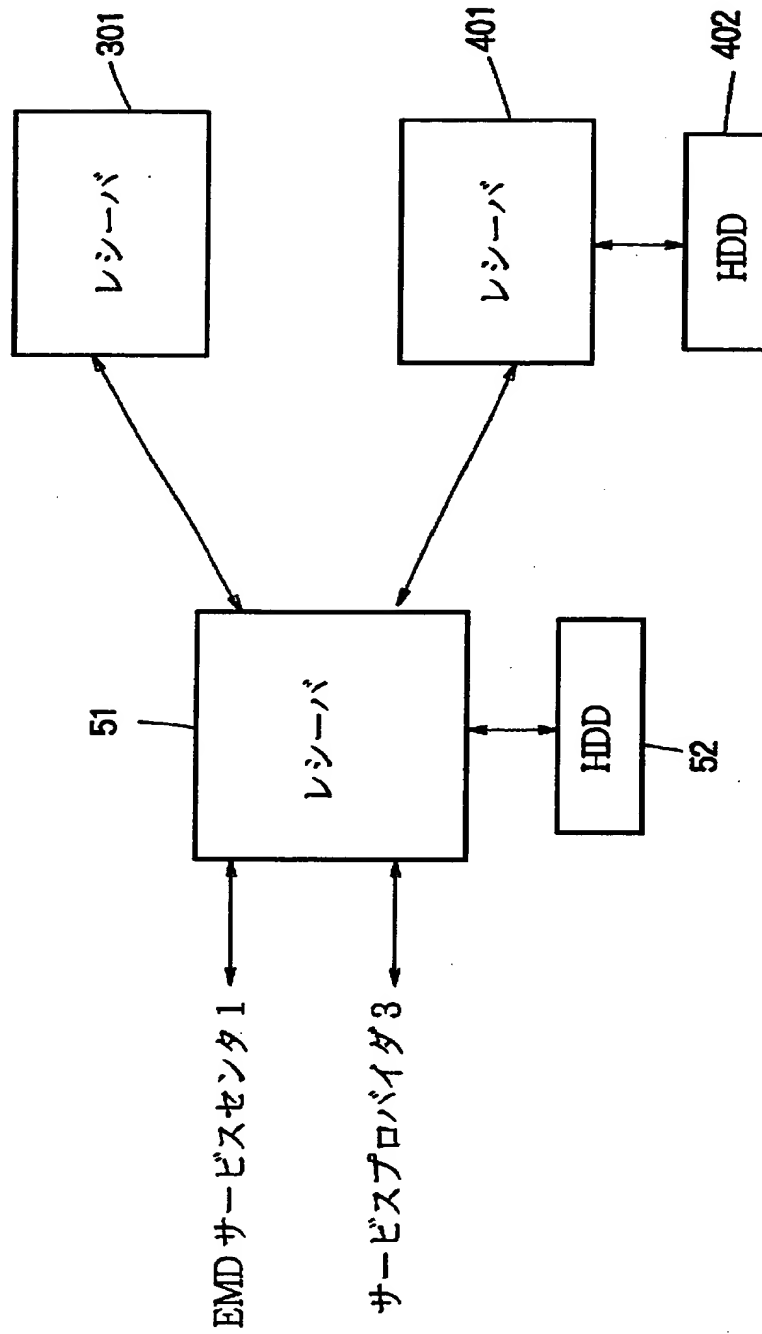


【図 50】

49-2

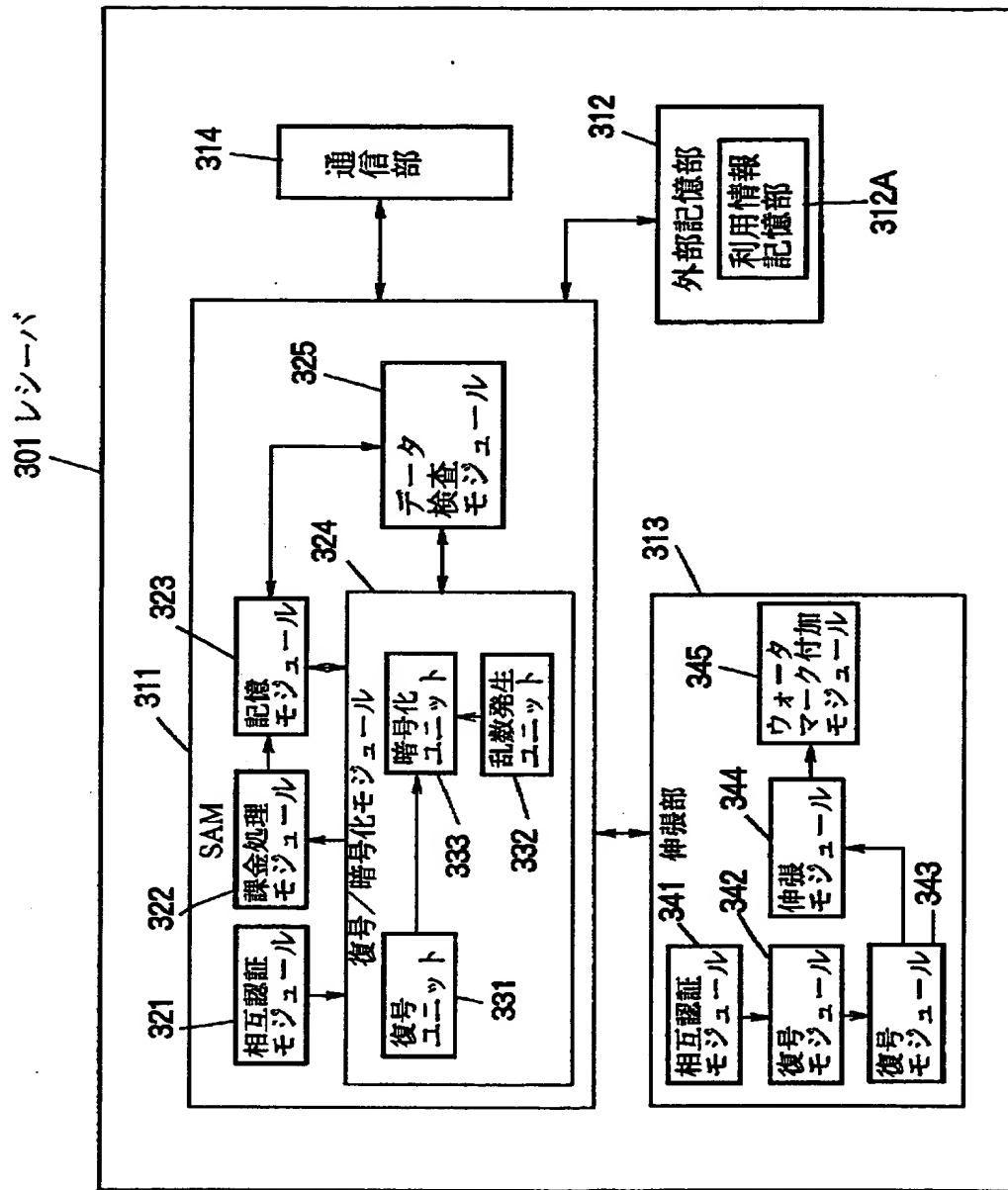


【図 52】

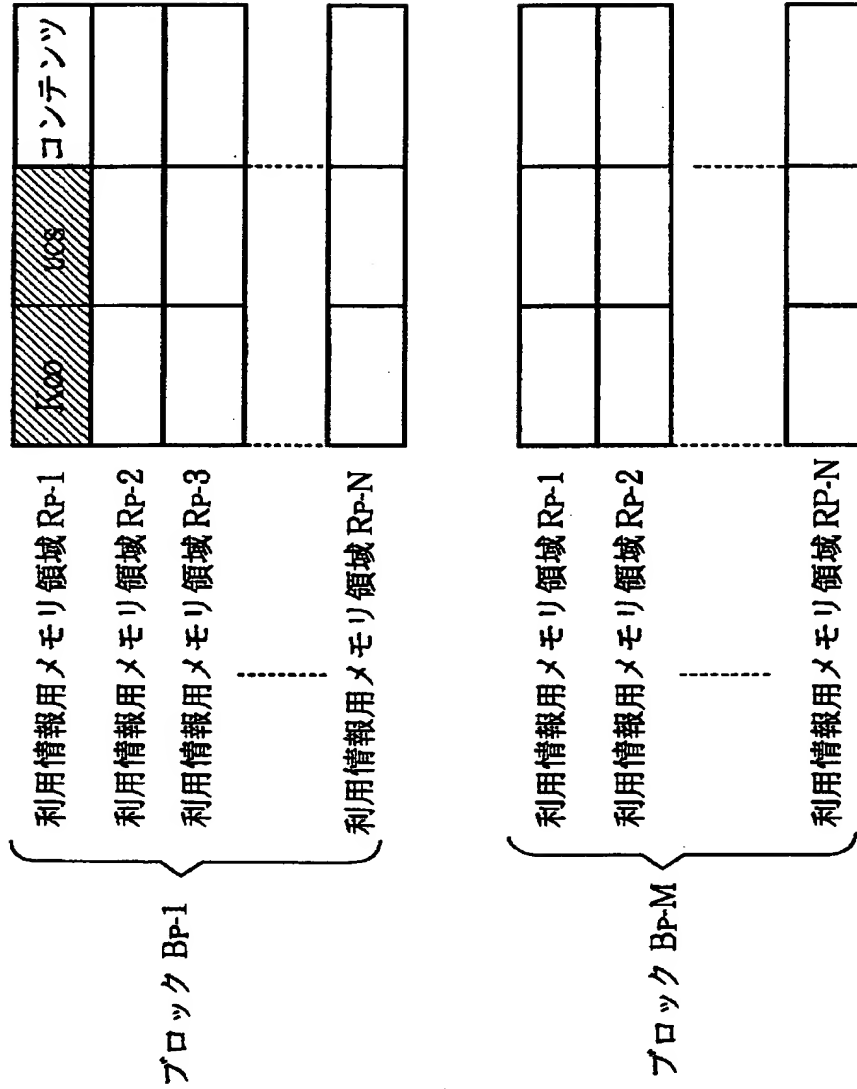


ユーザホームネットワーク 5

【図 5 3】



【図 5 4】



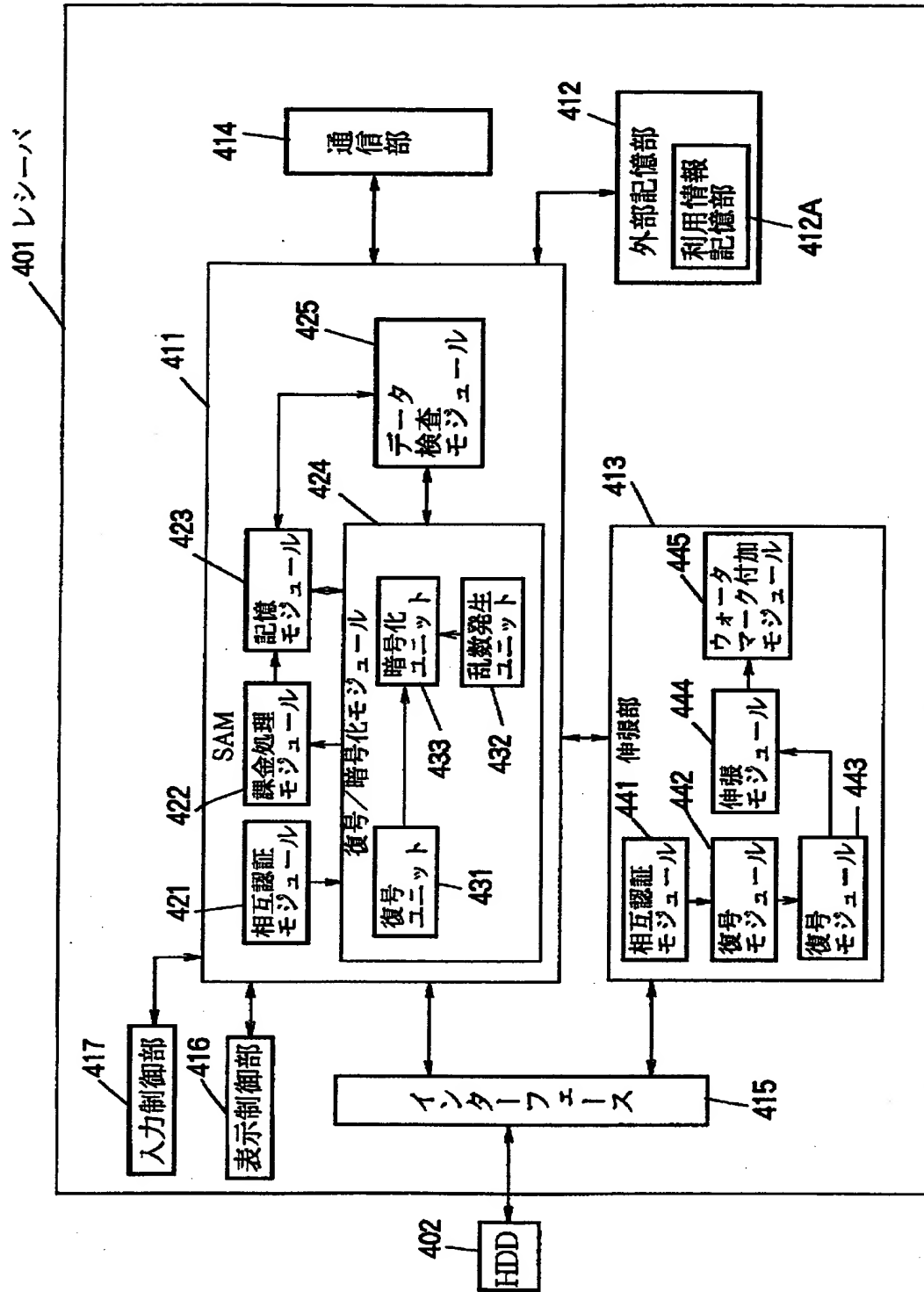
利用情報記憶部 312A

【図 5 5】

リスト部							
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名
SAM311のID	ユーザのID	不可	不可	なし	SAM62のID	制限なし	XXXX
登録リスト署名							
対象 SAM ID							
有効期限							
バージョン番号							
接続されている機器数							
SAM311 の ID							
XXXX							
XXXX							
2							

レシーバ 301 の登録リスト

【図 56】



【図 57】

レシーバ
401 の登録
条件

リスト部								
SAM ID	ユーザ ID	購入 処理	課金 処理	課金機器	コンテンツ 供給機器	状態 フラグ	登録条件 署名	登録リス ト署名
SAM411 の ID	ユーザの ID	不可	不可	なし	SAM62 の ID	制限 なし	×××××	××××

対象 SAM ID	SAM411 の ID	対象 SAM 情報部		
有効期限	××××			
バージョン番号	××××			
接続されている機器数	2			

レシーバ 401 の登録リスト

【図 5 8】

リスト部									
SAM ID	ユーザ ID	購入処理	課金処理	課金機器	コンテンツ供給機器	状態フラグ	登録条件署名	登録リスト署名	
レシーバ51の登録条件 SAM62のID	ユーザのID	可	可	SAM62のID	なし	制限なし	××××	××××	
レシーバ301の登録条件 SAM311のID	ユーザのID	不可	不可	なし	SAM62のID	制限なし	××××		
レシーバ401の登録条件 SAM411のID	ユーザのID	不可	不可	なし	SAM62のID	制限なし	××××		

対象 SAM ID

有効期限

バージョン番号

接続されている機器数

SAM62の ID

××××

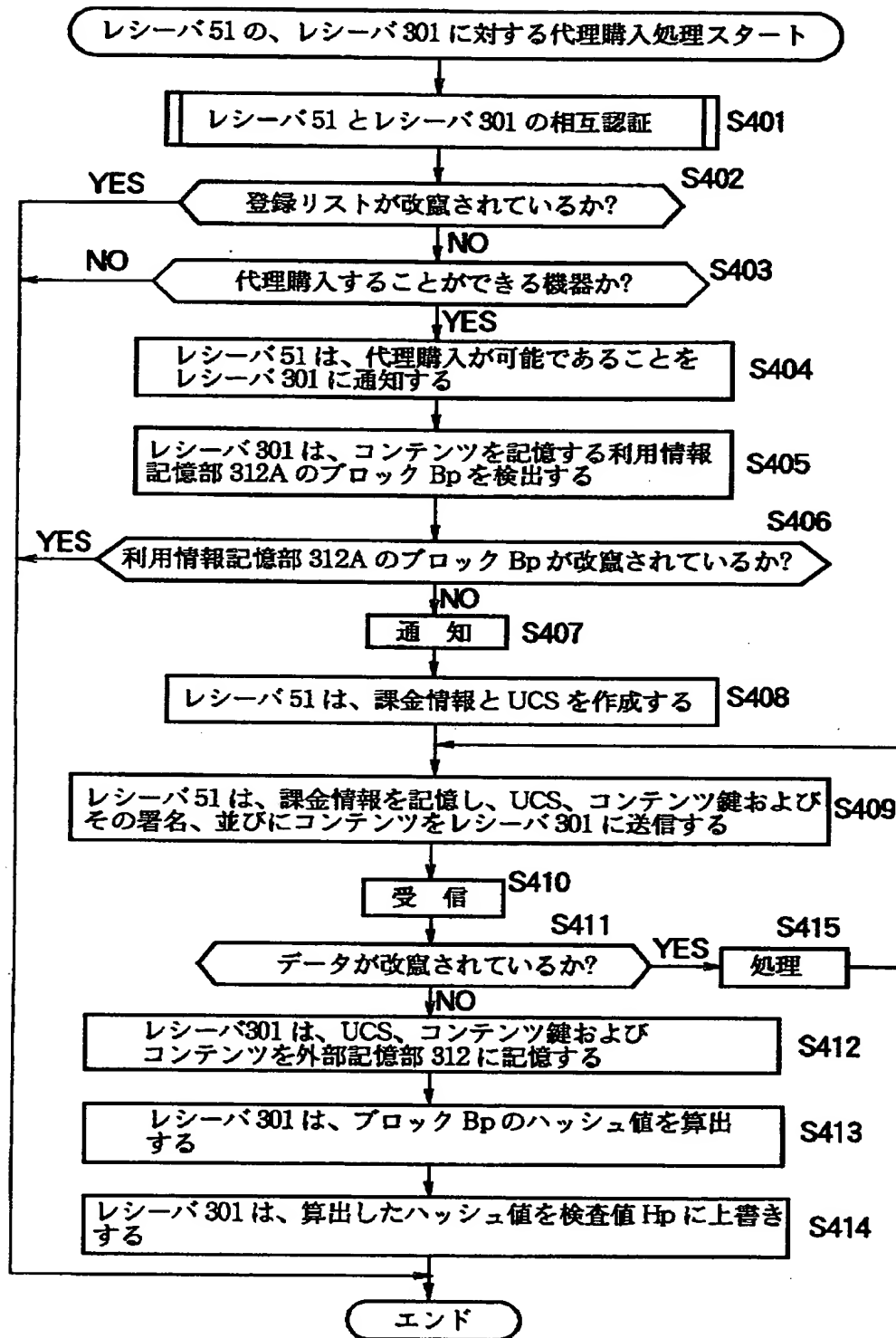
××××

3

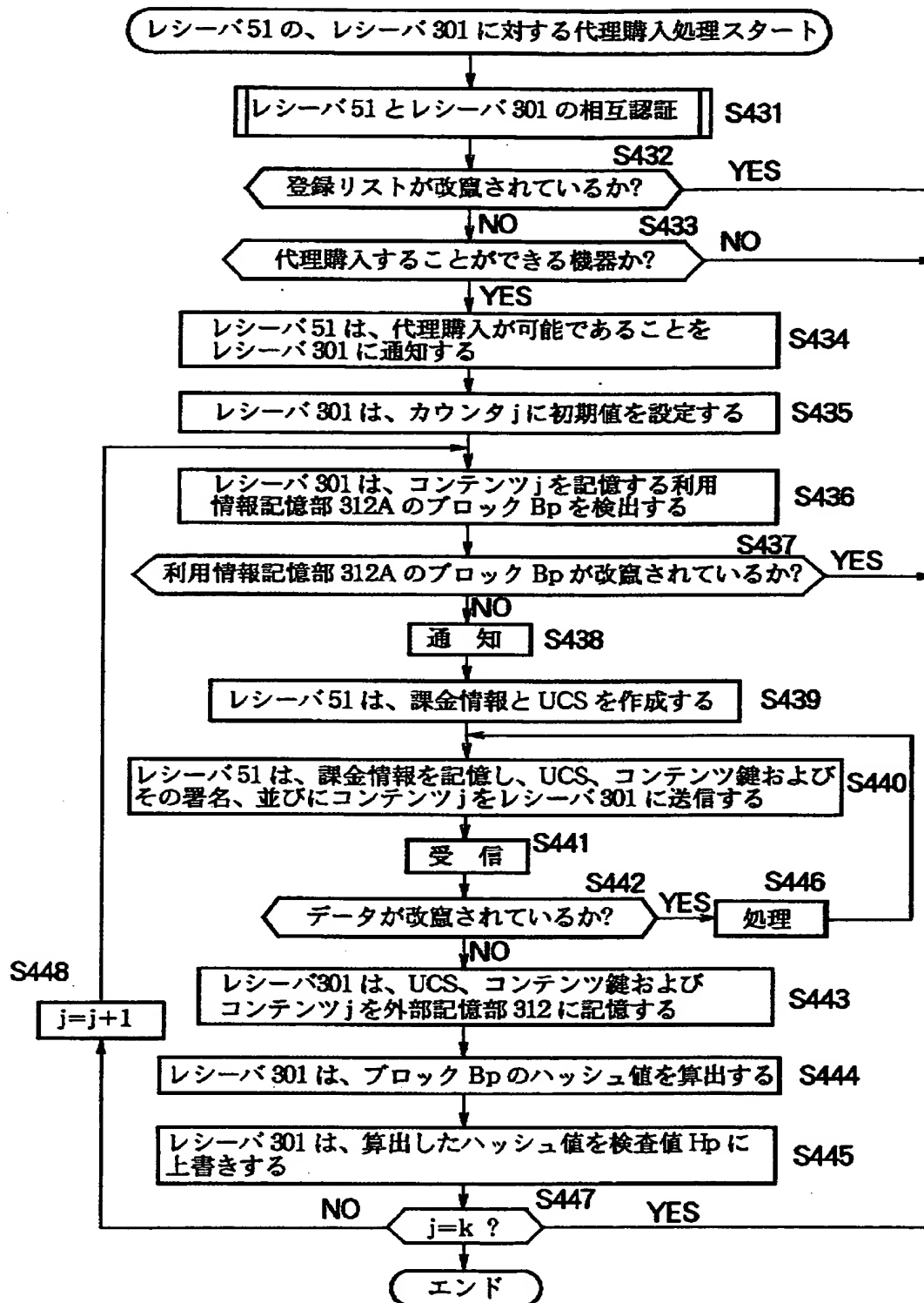
対象 SAM 情報部

登録リスト

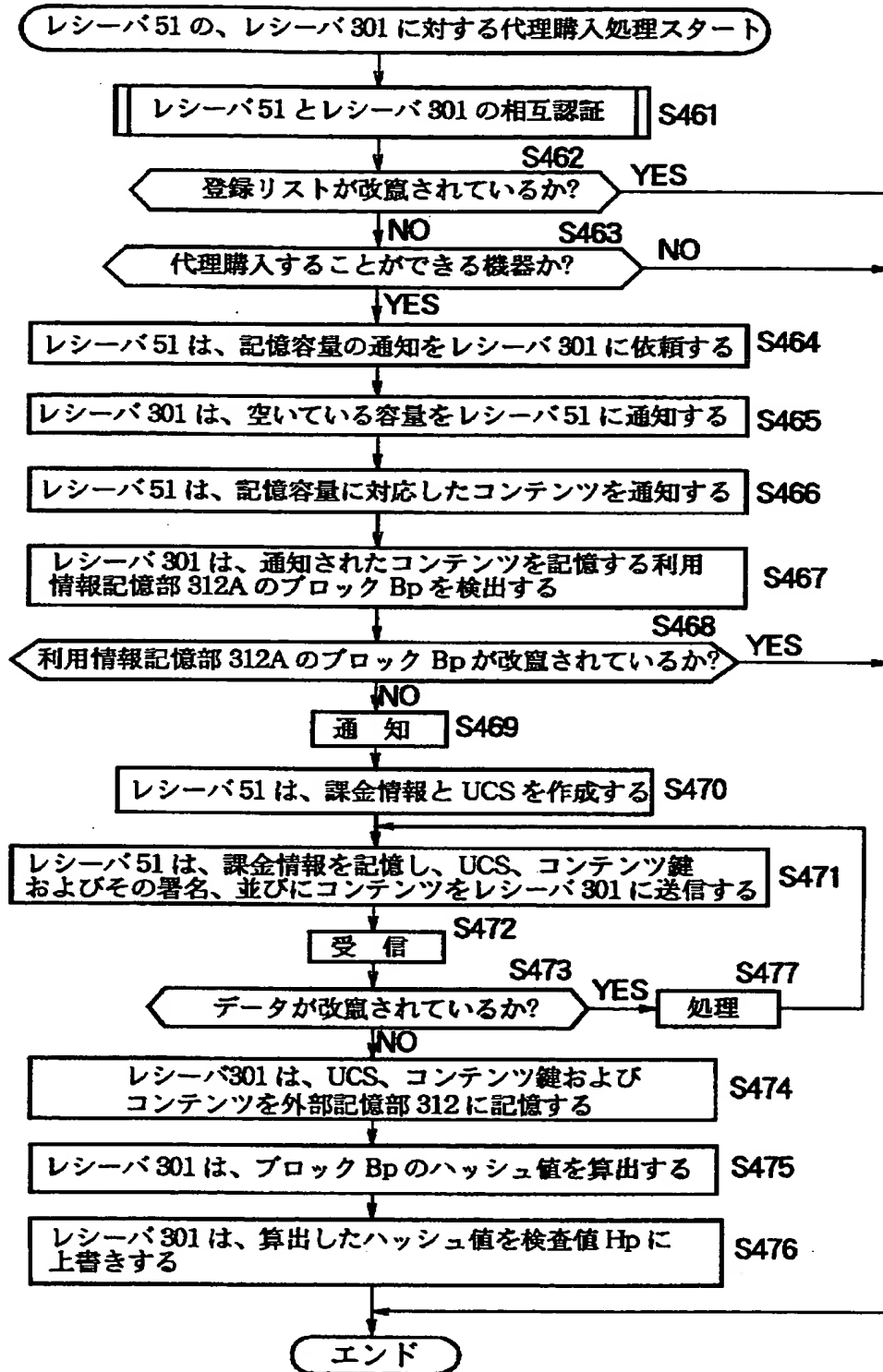
【図 59】



【図 60】

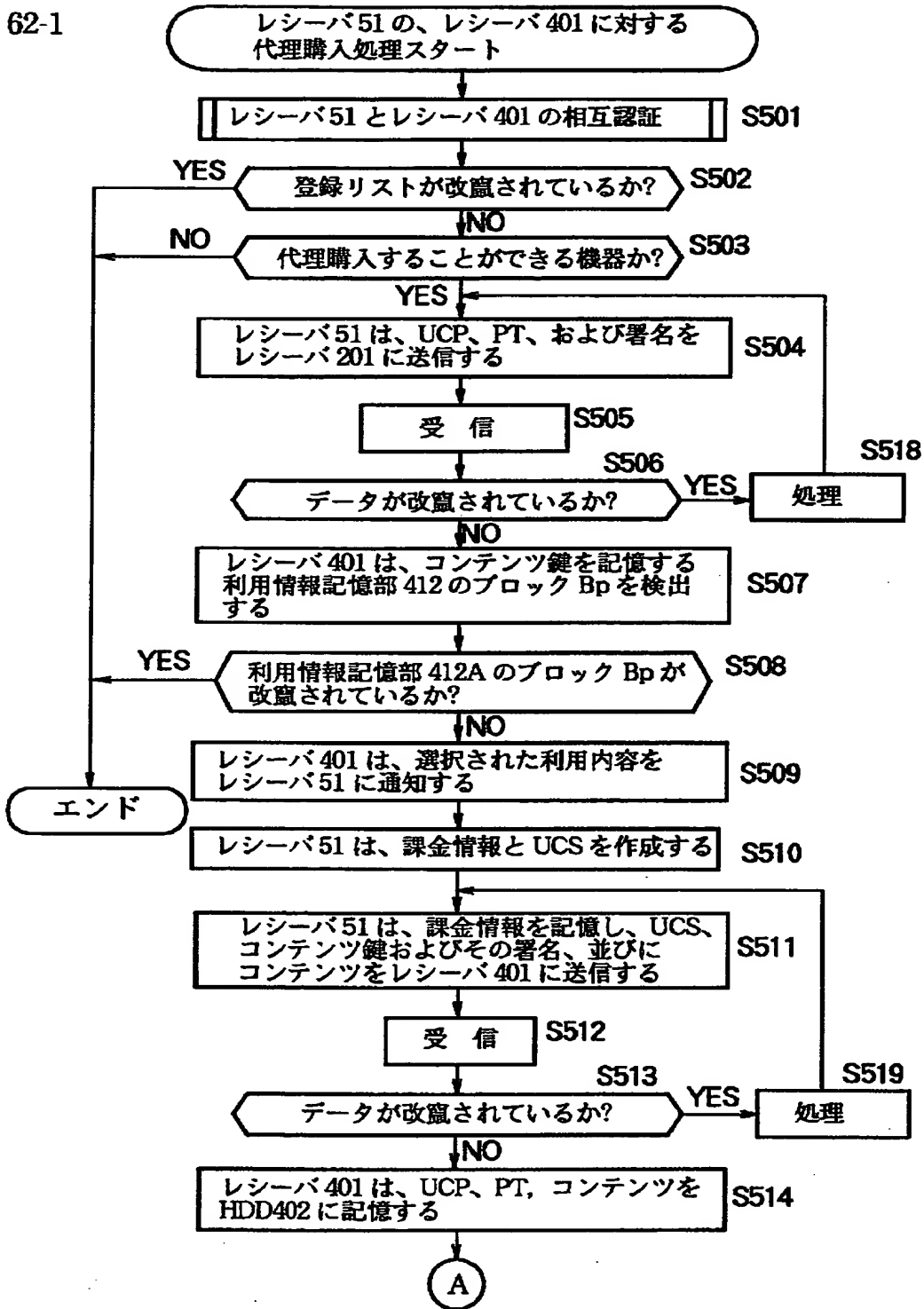


【図 6 1】



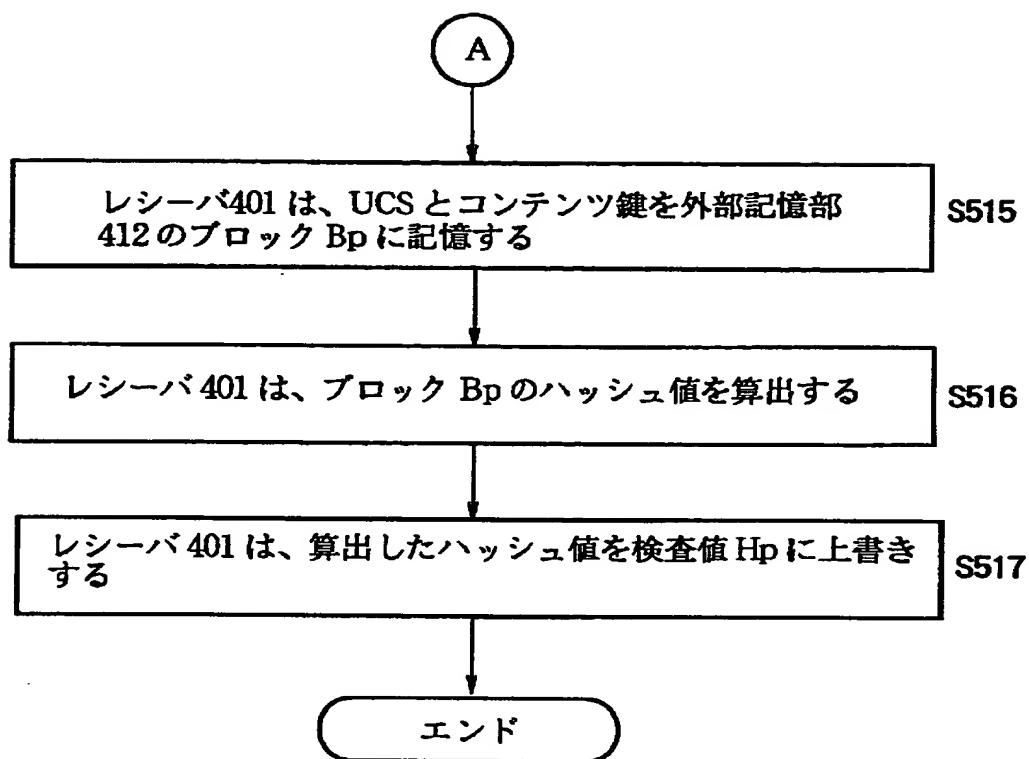
【図 6 2】

62-1



【図 63】

62-2



【書類名】 要約書

【要約】

【課題】 主の情報処理装置が、それに接続される情報処理装置に代わって、課金を決済する処理を行うことができるようにする。

【解決手段】 課金を決済する処理を行うことができないレシーバ201に代わって、レシーバ201において計上された課金を決済する処理を、レシーバ51が行う。

【選択図】 図1

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日	1990年 8月30日
[変更理由]	新規登録
住 所	東京都品川区北品川6丁目7番35号
氏 名	ソニー株式会社